

Aaron M. Sheanin (SBN 214472)
asheanin@robinskaplan.com
Christine S. Yun Sauer (SBN 314307)
cyunsauer@robinskaplan.com
ROBINS KAPLAN LLP
46 Shattuck Square, Suite 22
Berkeley, CA 94704
Telephone: (650) 784-4040
Facsimile: (650) 784-4041

*Attorneys for Plaintiffs
and the Proposed Classes*

[Additional counsel on signature page]

**UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA**

DEBORAH WESCH, DARIUS CLARK, JOHN
H. COTTRELL, WILLIAM B. COTTRELL,
RYAN HAMRE, GREG HERTIK, DAISY
HODSON, DAVID LUMB, KYLA ROLLIER
and JENNY SZETO, individually and on behalf
of all others similarly situated,

Plaintiff,

v.

YODLEE, INC., a Delaware corporation, and
ENVESTNET, INC., a Delaware corporation,

Defendants.

Case No.: 3:20-cv-05991-SK

**AMENDED CLASS ACTION
COMPLAINT**

JURY TRIAL DEMANDED

TABLE OF CONTENTS

	<u>Page</u>
SUMMARY OF ALLEGATIONS	1
JURISDICTION AND VENUE.....	4
PARTIES	4
I. Plaintiffs.....	4
II. Defendants	7
FACTUAL BACKGROUND.....	7
I. The Founding of Yodlee	7
II. Yodlee Collects and Sells Individuals’ Financial Data Without Their Consent	9
III. Yodlee’s Failure to Disclose Violates Several Privacy Laws.....	14
IV. Government and Industry Leaders Agree that Defendants’ Conduct Is Wrong, Risky, Dangerous and Bad for Consumers.....	17
INJURY AND DAMAGES TO THE CLASS	19
I. Plaintiffs and Class Members Have Suffered Economic Damages	20
II. Plaintiffs Have Lost Control Over Valuable Property	20
III. Yodlee Does Not Have Adequate Safeguards to Protect Consumers’ Data	23
IV. Congress Has Requested an FTC Investigation into Envestnet & Yodlee Practices	26
TOLLING, CONCEALMENT AND ESTOPPEL	27
CLASS ACTION ALLEGATIONS	28
CALIFORNIA LAW APPLIES TO THE NATIONWIDE CLASS.....	30
CLAIMS FOR RELIEF	31

Deborah Wesch, Darius Clark, John H. Cottrell, William B. Cottrell, Ryan Hamre, Greg Hertik, Daisy Hodson, David Lumb, Kyla Rollier and Jenny Szeto (together, “Plaintiffs”), on behalf of themselves and all others similarly situated, assert the following against Defendants Yodlee, Inc., (“Yodlee”) and Envestnet Inc., (“Envestnet”) (collectively “Defendants”), based upon personal knowledge, where applicable, information and belief, and the investigation of counsel.

SUMMARY OF ALLEGATIONS

1. The Internet age has spawned the development of a vast data economy. Among its key players are data aggregators, companies that collect and repackage data from various sources for sale to advertisers, investors, researchers, and other third parties.

2. Yodlee is one of the largest financial data aggregators in the world. Its business focuses on selling highly sensitive financial data, such as bank balances and credit card transaction histories, collected from individuals throughout the United States. For example, as Yodlee’s former chief product officer explained in a 2015 interview, “‘Yodlee can tell you down to the day how much the water bill was across 25,000 citizens of San Francisco,’ or the daily spending at McDonald’s throughout the country.’”¹

3. This data is not available from public sources and is so sensitive that the individuals it concerns would not voluntarily turn it over.

4. Rather, Yodlee surreptitiously collects such data from software products that it markets and sells to some of the largest financial institutions in the country. These institutions, including 15 top banks (e.g., Bank of America, Merrill Lynch, and Citibank), 10 top wealth management firms, and digital payment platforms like PayPal, use Yodlee’s software for various purposes, including to connect their systems to one another.

5. Yodlee, in turn, acquires financial data about each individual that interacts with the software installed on its customers’ systems. However, these individuals often have no idea they

¹ Bradley Hope, *Provider of Personal Finance Tools Tracks Bank Cards, Sells Data to Investors*, WALL ST. J. (Aug. 6, 2015), <https://www.wsj.com/articles/provider-of-personal-finance-tools-tracks-bank-cards-sells-data-to-investors-1438914620>.

1 are dealing with Yodlee.

2 6. This is by design. Given the highly sensitive nature of the data Yodlee collects,
3 Yodlee's software is developed to be seamlessly integrated directly into the host company's
4 existing website and/or mobile app in a way that obscures who the individual is dealing with and
5 where their data is going. For example, when individuals connect their bank accounts to PayPal,
6 they are prompted to enter their credentials into a log in screen that mirrors what they would see
7 if they directly logged into their respective bank's website. *See* Factual Background Part II, below.
8 Their financial institution's logo is prominently displayed on each of the screens that they interact
9 with and the individuals use the same usernames and passwords they would use to log in to their
10 financial institution's own website or mobile app. At no point are the individuals prompted to
11 create or use a Yodlee account.

12 7. Moreover, to the extent Yodlee is mentioned, individuals are not given accurate
13 information about what Yodlee does or how it collects their data. For example, PayPal discloses
14 to individuals that Yodlee is involved in connecting their bank account to PayPal's service for the
15 limited purpose of confirming the individual's bank details, checking their balance, and
16 transactions, as needed. While this might be true for that initial log in, Yodlee's involvement with
17 the individual's data goes well beyond the limited consent provided to facilitate a connection
18 between their bank account and PayPal.

19 8. Yodlee, in fact, stores a copy of each individual's bank log in information (i.e., her
20 username and password) on its own system *after* the connection is made between that individual's
21 bank account and any other third party service (e.g., PayPal).

22 9. Yodlee then exploits this information to routinely extract data from that user's
23 accounts without their consent.

24 10. This process continues even if, for example, an individual severs the connection
25 between its bank account and the third-party service (e.g., PayPal) that Yodlee facilitated. In that
26 instance, Yodlee relies on its own stored copy of the individual's credentials to extract financial
27 data from her accounts long after the access is revoked.

28 11. This unagreed-to data collection is particularly problematic because "[c]onsumers'

1 credit and debit card transactions can reveal information about their health, sexuality, religion,
 2 political views, and many other personal details.”² It is no wonder that Yodlee has been highly
 3 successful as, according to the *Wall Street Journal*, companies are willing to pay as much as \$4
 4 million a year for access to this sort of highly personal data.

5 12. Plaintiffs connected their bank accounts to PayPal using a Yodlee-powered portal
 6 in order to facilitate transfers among those accounts. At no time was it disclosed by PayPal, Yodlee,
 7 or the banks that the Defendants would continuously access Plaintiffs’ accounts to extract and sell
 8 data without their consent.

9 13. This is especially troubling as reports have revealed that Defendants are
 10 mishandling the data they collected from individuals without authorization by distributing it in
 11 unencrypted plain text files. These files, which can be read by anyone who acquires them, contain
 12 highly sensitive information that make it possible to identify the individuals involved in each
 13 transaction.

14 14. Yodlee’s failure to take even the most basic steps to protect this highly sensitive
 15 data (e.g., requiring a password to open such files) has placed Plaintiffs and all Class members at
 16 significant risk of fraud and identity theft. This risk is especially heightened given Yodlee’s
 17 practice of reselling the data it collects—without authorization—to third parties. While Yodlee
 18 claims to protect this data while in its custody, it has admitted in filings with the United States
 19 Securities and Exchange Commission (“SEC”) that it “does not audit its customers to ensure that
 20 they have acted, and continue to act, consistently with such assurances.”³ Yodlee, accordingly,
 21 cannot guarantee Plaintiffs or other Class members that its clients, or anyone with whom its clients
 22 share Class members’ sensitive personal data, are not using such data for nefarious purposes.

23 15. Given Defendants’ secretive data collection practices and recent reports regarding
 24

25 ² Letter from Senator Ron Wyden et al, Cong. of the U.S., to Joseph J. Simons, Chairman, Fed.
 26 Trade Comm’n (Jan. 17, 2020),
 27 <https://www.wyden.senate.gov/imo/media/doc/011720%20Wyden%20Brown%20Eshoo%20Env%20Yodlee%20Letter%20to%20FTC.pdf>.

28 ³*Proxy Statement/Prospectus*, Yodlee (Oct. 21, 2015),
<https://www.sec.gov/Archives/edgar/data/1337619/000104746915007906/a2226277z424b3.htm>.

its grossly inadequate approach to data security, Plaintiffs believe that additional evidence supporting its claims will be uncovered following a reasonable opportunity for discovery.

JURISDICTION AND VENUE

16. Pursuant to 28 U.S.C. § 1331, this Court has original subject matter jurisdiction over the claims that arise under the Computer Fraud and Abuse Act, 18 U.S.C. § 1030, and the Stored Communications Act, 18 U.S.C. § 2701. This Court has supplemental jurisdiction over all other claims pursuant to 28 U.S.C. § 1367(a).

17. This Court also has jurisdiction over the subject matter of this action pursuant to 28 U.S.C. § 1332(d), because the amount in controversy for the Class exceeds \$5,000,000 exclusive of interest and costs, there are more than 100 putative members of the Classes defined below, and a significant portion of putative Class members are citizens of a state different from Defendants.

18. This Court has general personal jurisdiction over Yodlee because Yodlee's principal place of business is in Redwood City, California.

19. This Court has specific personal jurisdiction over Envestnet because it regularly conducts business in this District and a substantial portion of the events and conduct giving rise to Plaintiffs' claims occurred in this State.

20. Venue is proper in this District pursuant to 28 U.S.C. § 1391(b), (c), and (d) because Defendants transact business in this District; a substantial portion of the events giving rise to the claims occurred in this District; and because Defendant Yodlee is headquartered in this District.

21. Intra-district Assignment: A substantial part of the events and omissions giving rise to the violations of law alleged herein occurred in the County of San Mateo, and as such, this action may be properly assigned to the San Francisco or Oakland divisions of this Court pursuant to Civil Local Rule 3-2(c).

PARTIES

I. PLAINTIFFS

22. Plaintiff **Deborah Wesch** is a natural person and citizen of the State of New Jersey and a resident of Monmouth County.

23. Ms. Wesch is a PayPal user who connected her PNC Bank account to PayPal

1 through Yodlee's account verification application programming interface ("API") in order to
2 facilitate transfers among those accounts. At no time was it disclosed by PayPal, Yodlee, or PNC
3 Bank that Defendants would continuously access Ms. Wesch's accounts to extract data.
4 Defendants abused their access to Ms. Wesch's accounts by collecting, retaining and selling her
5 data without her knowledge or consent.

6 24. Plaintiff **Darius Clark** is a natural person, a citizen of the State of Ohio and a
7 resident of Hamilton County.

8 25. Mr. Clark is a PayPal user who connected his Alliant Credit Union, UMB/Fidelity,
9 and BBVA Simple accounts to PayPal through Yodlee's API in order to facilitate transfers among
10 those accounts. At no time was it disclosed by PayPal, Yodlee, Alliant Credit Union, UMB/Fidelity,
11 or BBVA Simple that Defendants would continuously access Mr. Clark's accounts to extract data.
12 Defendants abused their access to Mr. Clark's accounts by collecting, retaining and selling his data
13 without his knowledge or consent.

14 26. Plaintiff **John H. Cottrell** is a natural person, a citizen of the State of Texas and a
15 resident of Collin County.

16 27. Mr. John Cottrell is a PayPal user who connected his Bancorp Bank account to
17 PayPal through Yodlee's API in order to facilitate transfers among those accounts. At no time was
18 it disclosed by PayPal, Yodlee, or Bancorp Bank that Defendants would continuously access Mr.
19 John Cottrell's accounts to extract data. Defendants abused their access to Mr. John Cottrell's
20 accounts by collecting, retaining and selling his data without his knowledge or consent.

21 28. Plaintiff **William B. Cottrell** is a natural person, a citizen of the State of Arkansas
22 and a resident of Hot Spring County.

23 29. Mr. William Cottrell is a PayPal user who connected his Bank of Little Rock
24 account to PayPal through Yodlee's API in order to facilitate transfers among those accounts. At
25 no time was it disclosed by PayPal, Yodlee, or Bank of Little Rock that Defendants would
26 continuously access Mr. William Cottrell's accounts to extract data. Defendants abused their
27 access to Mr. William Cottrell's accounts by collecting, retaining and selling his data without his
28 knowledge or consent.

1 30. Plaintiff **Ryan Hamre** is a natural person, a citizen of the State of Maine and a
2 resident of Knox County.

3 31. Mr. Hamre is a PayPal user who connected his Chase, BBVA and TD Bank
4 accounts to PayPal through Yodlee's API in order to facilitate transfers among those accounts. At
5 no time was it disclosed by PayPal, Yodlee, Chase, BBVA or TD Bank that Defendants would
6 continuously access Mr. Hamre's accounts to extract data. Defendants abused their access to Mr.
7 Hamre's accounts by collecting, retaining and selling his data without his knowledge or consent.

8 32. Plaintiff **Greg Hertik** is a natural person and citizen of the State of Georgia and a
9 resident of Forsyth County.

10 33. Mr. Hertik is a PayPal user who connected his USAA account to PayPal through
11 Yodlee's API in order to facilitate transfers among those accounts. At no time was it disclosed by
12 PayPal, Yodlee, or USAA that Defendants would continuously access Mr. Hertik's accounts to
13 extract data. Defendants abused their access to Mr. Hertik's accounts by collecting, retaining and
14 selling his data without his knowledge or consent.

15 34. Plaintiff **Daisy Hodson** is a natural person, a citizen of the State of Utah and a
16 resident of Salt Lake County.

17 35. Ms. Hodson is a PayPal user who connected her Wells Fargo account to PayPal
18 through Yodlee's API in order to facilitate transfers among those accounts. At no time was it
19 disclosed by PayPal, Yodlee, or Wells Fargo that Defendants would continuously access Ms.
20 Hodson's accounts to extract data. Defendants abused their access to Ms. Hodson's accounts by
21 collecting, retaining and selling her data without her knowledge or consent.

22 36. Plaintiff **David Lumb** is a natural person, a citizen of the State of Tennessee and a
23 resident of Shelby County.

24 37. Mr. Lumb is a PayPal user who connected his Commercial Bank & Trust account
25 to PayPal through Yodlee's API in order to facilitate transfers among those accounts. At no time
26 was it disclosed by PayPal, Yodlee, or Commercial Bank & Trust that Defendants would
27 continuously access Mr. Lumb's accounts to extract data. Defendants abused their access to Mr.
28 Lumb's accounts by collecting, retaining and selling his sensitive personal data without his

1 knowledge or consent.

2 38. Plaintiff **Kyla Rollier** is a natural person and citizen of the State of Florida and a
3 resident of Volusia County.

4 39. Ms. Rollier is a PayPal user who connected her Launch Credit Union account to
5 PayPal through Yodlee's API in order to facilitate transfers among those accounts. At no time was
6 it disclosed by PayPal, Yodlee, or Launch Credit Union that Defendants would continuously access
7 Ms. Rollier's accounts to extract data. Defendants abused their access to Ms. Rollier's accounts
8 by collecting, retaining and selling her data without her knowledge or consent.

9 40. Plaintiff **Jenny Szeto** is a natural person and citizen of the State of California and
10 a resident of San Francisco County.

11 41. Ms. Szeto is a PayPal user who connected her J.P. Morgan Chase account to PayPal
12 through Yodlee's API in order to facilitate transfers among those accounts. At no time was it
13 disclosed by PayPal, Yodlee, or J.P. Morgan Chase that Defendants would continuously access
14 Ms. Szeto's accounts to extract data. Defendants abused their access to Ms. Szeto's accounts by
15 collecting, retaining and selling her data without her knowledge or consent.

16 **II. DEFENDANTS**

17 42. Defendant Yodlee, Inc. is a Delaware corporation with principal executive offices
18 located at 3600 Bridge Parkway, Suite 200, Redwood City, CA 94065.

19 43. Defendant Envestnet, Inc. is a Delaware corporation, with principal executive
20 offices located at 35 East Wacker Drive, Suite 2400, Chicago, Illinois 60601.

21 **FACTUAL BACKGROUND**

22 **I. THE FOUNDING OF YODLEE**

23 44. Yodlee was founded in 1999. Initially, Yodlee was focused on providing banks and
24 financial institutions with software that would improve the user experience, for example, making
25 it possible for banking clients to view bank statements, financial accounts, and investment
26 portfolios all at once without relying on multiple logins or webpages.

27 45. Yodlee later expanded its business to develop APIs for financial apps and software
28 (collectively, "FinTech Apps"). This includes payment apps, such as Paypal; personal budgeting

1 apps, such as Personal Capital; and apps for particular banks. Yodlee's software silently integrates
2 into its clients' existing platforms to provide various financial services, like budgeting tools,
3 savings trackers, or account history information. In each instance, the customer believes that it is
4 interacting with its home institution (e.g., its bank) and has no idea it is logging into or using a
5 Yodlee product.

6 46. Defendants profit from these interactions in two ways. First, the financial
7 institutions that use Defendants' software pay a licensing fee to integrate Yodlee's API into their
8 platform. Second, Yodlee collects the financial data of each individual that connects to one of the
9 FinTech Apps through a bank or other financial institution using its software. This information,
10 which includes bank account balances, transaction history and other data, is then aggregated with
11 that of other individuals and sold to third parties for a fee.

12 47. Yodlee's reach and the amount of data it collects is extraordinary. More than 150
13 financial institutions and a majority of the 20 largest U.S. banks integrate Defendants' API into
14 their platforms. According to filings with the SEC, more than 900 companies subscribe to the
15 Yodlee platform to power customized FinTech Apps and services for millions of their users.

16 48. Given its widespread success, Yodlee went public on NASDAQ in October of 2014,
17 generating almost \$100 million that year. Prior to its public offering, Yodlee claims it only
18 provided data to third parties for "research uses," such as "enhanc[ing] predictive analysis."

19 49. In 2015, Yodlee was acquired by Envestnet. The deal valued Yodlee at \$590 million
20 or approximately \$19 per share. The acquisition was considered the second largest FinTech deal
21 in U.S. history at the time.

22 50. That same year, the *Wall Street Journal* released a report revealing for the first time
23 that a large part of Yodlee's revenue was actually generated by a different lucrative source: selling
24 user data. The report concluded that Yodlee has been selling data it gathers from users for at least
25 the last year.

26 51. Yodlee denied the *Wall Street Journal* report, claiming it had only "a very limited
27 number of partnerships with firms to develop . . . sophisticated analytics solutions." Yodlee
28 claimed these partners only received "a small, scrubbed, de-identified, and dynamic sample of data

1 to enable trend analysis. Yodlee does not offer, nor do partners receive, raw data.”

2 52. Currently, Defendants sell sensitive personal data of tens of millions of individuals
3 to a large customer base, including investment firms and some of the largest banks in the United
4 States, like J.P. Morgan.⁴ One of Yodlee’s products, called its “Data Platform,” offers “the best
5 and most comprehensive financial data at massive scale across retail banking, credit, and wealth
6 management.” Yodlee explains “[t]his is made possible through the strengths of our data
7 acquisition capabilities, extensive data cleaning and enrichment expertise, and massive scale.”⁵

8 53. Defendants’ sale of users’ highly sensitive personal data violates their privacy
9 rights and several state and federal laws because, as explained below, that data is collected without
10 Plaintiffs’ and Class members’ knowledge or consent. Furthermore, Yodlee fails to implement
11 adequate security measures to protect Plaintiffs’ and Class members’ data, leaving their highly
12 sensitive personal data vulnerable to hackers, criminals, and other unauthorized third parties.

13 **II. YODLEE COLLECTS AND SELLS INDIVIDUALS’ FINANCIAL DATA** 14 **WITHOUT THEIR CONSENT**

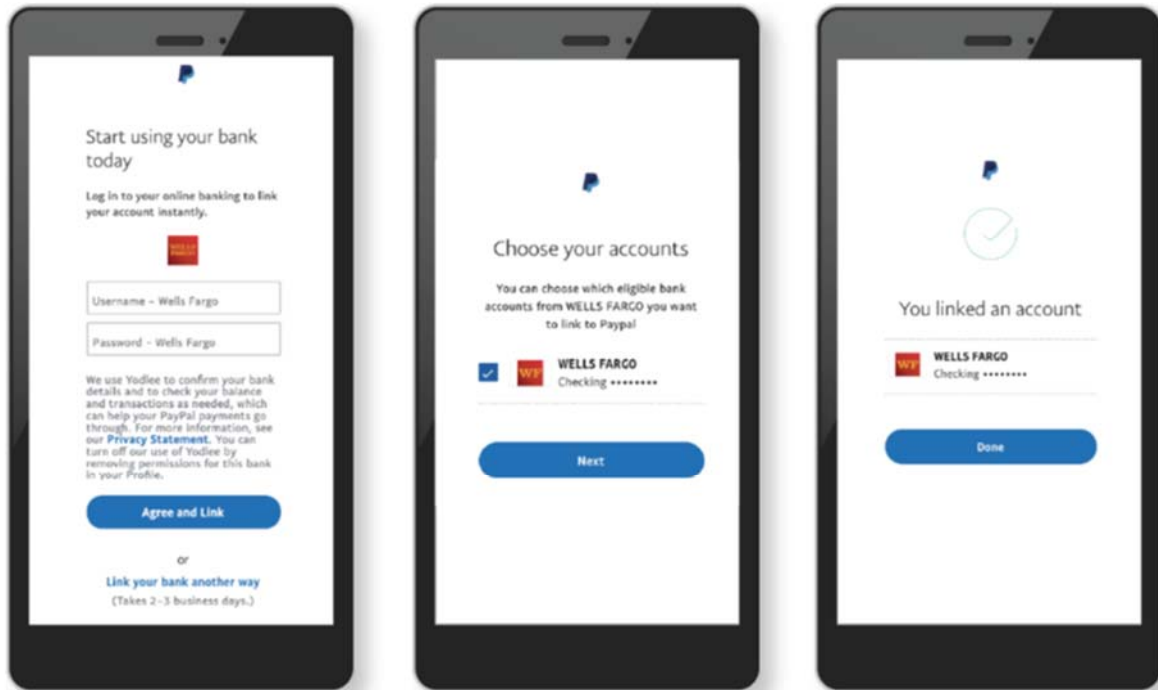
15 54. While Yodlee claims that it only sells “small . . . sample[s] of data,”⁶ in reality,
16 Defendants sell millions of users’ sensitive personal data to hundreds of clients. As explained
17 below, this data is collected without the individual’s consent by leveraging credentials provided to
18 Yodlee for a different, specific, and limited purpose.

19 55. For example, PayPal uses Yodlee’s account verification API to validate an
20 individual’s bank account so that the individual can use that account with PayPal’s services. An
21 individual is prompted by the following screen when attempting to connect her bank account:

24 ⁴ Joseph Cox, *Leaked Document Shows How Big Companies Buy Credit Card Data on Millions*
25 *of Americans*, VICE, (Feb. 19, 2017), [https://www.vice.com/en_us/article/jged4x/envestnet-](https://www.vice.com/en_us/article/jged4x/envestnet-yodlee-credit-card-bank-data-not-anonymous)
26 [yodlee-credit-card-bank-data-not-anonymous](https://www.vice.com/en_us/article/jged4x/envestnet-yodlee-credit-card-bank-data-not-anonymous).

27 ⁵ *Id.*

28 ⁶ *Yodlee Responds and Corrects The Wall Street Journal Article*, YODLEE, archived at:
<https://web.archive.org/web/20150816230052/https://www.yodlee.com/yodlee-responds/> (last
visited Aug. 21, 2020).

FIGURE 1

56. The first screen displayed in Figure 1 states that “[PayPal] use[s] Yodlee to confirm your bank details and to check your balance and transaction as needed, which can help your PayPal payments go through.” This limited interaction is all that the individual consents to. Nowhere does she give either PayPal or Yodlee permission to collect and store data for resale.

57. But this is exactly what happens. Yodlee goes beyond facilitating the log in transactions by storing a copy of the individual’s banking data, and retains the username and password that the individual provides on log in screens, like that displayed in Figure 1, to collect and store the individual’s bank account transaction history on an ongoing basis. The individual never consents to this kind of data collection, which solely benefits Yodlee and is unrelated and unnecessary to complete the log in transaction.

58. An individual cannot opt out of or turn off Yodlee’s access to her bank account information after providing her credentials. For example, while the first screen in Figure 1 states, “[y]ou can turn off our use of Yodlee by removing permissions for this Bank in your Profile,” this pertains only to PayPal’s access. Yodlee still retains the individual’s credentials and continues to access her bank account to collect and sell highly sensitive financial data without consent even

1 after PayPal's permissions are removed.

2 59. Yodlee's recurring collection of and continued access to an individual's financial
3 data is never disclosed. Yodlee's privacy policy only applies to its own direct-to-consumer
4 products and does not cover the APIs that power FinTech Apps or facilitate log in transactions like
5 that described in Figure 1.⁷ Instead, Yodlee directs an individual using "Yodlee powered services
6 delivered through a Yodlee client" to refer to Defendants' "client's data governance and privacy
7 practices." Thus, where an individual unknowingly uses Yodlee to connect her bank accounts to a
8 FinTech App, there is nowhere she could have looked in *Yodlee's* policies to learn the full extent
9 of data Defendants were collecting from her or the fact that Defendants were selling her data.

10 60. Nor does Yodlee require its FinTech App clients to make any such disclosures. For
11 example, while the PayPal Privacy Statement linked to in the first screen of Figure 1 discloses that
12 PayPal does not "sell [individuals'] personal data," it says nothing about whether third-party
13 service providers, such as Yodlee, collect and sell such sensitive financial data. Likewise, while
14 the PayPal Privacy Statement provides that "you *may* be able to manage how your personal data
15 is collected, used, and shared by [third-parties]," it does not provide individuals with a way to
16 manage what data Defendants collect about them through PayPal or how Defendants use and share
17 that data with others. Such controls would have to come directly from Yodlee, which does not
18 allow individuals to manage their personal data, because doing so would undermine Defendants'
19 highly profitable data aggregation business.

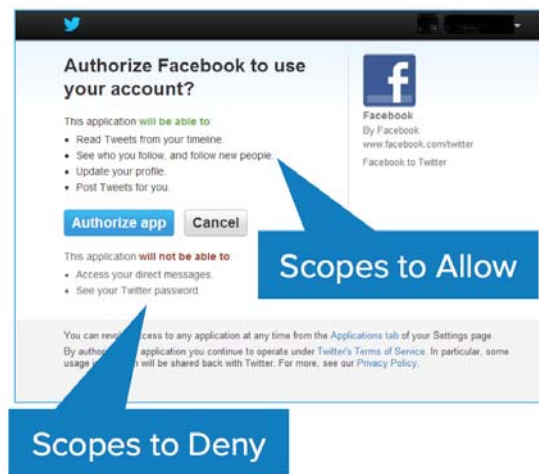
20 61. Not only do Defendants collect more data than is necessary from individuals that
21 interact with their FinTech Apps—Defendants' service is not necessary at all.

22 62. Historically, in order to allow a third party access to a bank account, a user had to
23 submit her bank routing and account numbers; transfer a small trial deposit (usually a few cents);
24 and then return to the bank to verify the amount transferred. This process usually took several days,
25 a delay that could—in the fast-moving Internet age—cause potential users of FinTech Apps to

27 ⁷ *Privacy Notice*, YODLEE (July 31, 2020), <https://www.yodlee.com/europe/legal/privacy-notice#:~:text=The%20Yodlee%20Services%20databases%20are,of%20identification%20including%20biometric%20authentication.>
28

1 give up on using the app at all.

2 63. One alternative to this process is “OAuth.” Users are likely familiar with this
 3 procedure because it has become the industry-standard protocol for users who wish to grant a
 4 website or an app permission to access certain information from another website or app. Crucially,
 5 OAuth “enables apps to obtain limited access (scopes) to a user’s data without giving away a user’s
 6 password.”⁸ For instance, consider an example in which a user wishes to grant Facebook
 7 permission to access her Twitter account so that it can integrate its social media accounts together.
 8 Before it can do so, the user will be redirected from Facebook to Twitter, where it must login to
 9 ensure it is authorized to grant those permissions.⁹ Then, a dialogue box pops up, asking which
 10 permissions the user is granting and which it is denying. The dialogue box might look something
 11 like this:¹⁰



12
 13
 14
 15
 16
 17
 18
 19
 20 64. In this example, note that the user grants Facebook permission to update its Twitter
 21 profile and even post to the user’s Twitter account (“This application will be able to . . . Update
 22 your profile; Post Tweets for you”), but *denies* Facebook permission to see the user’s Twitter
 23 password (“This application will not be able to . . . See your Twitter password”). Instead, the user
 24

25
 26 ⁸ See Matt Raible, *What the Heck is OAuth?* OKTA (June 21, 2017),
<https://developer.okta.com/blog/2017/06/21/what-the-heck-is-oauth>.

27 ⁹ Redirection from the app the user is currently using to the app where it retains the data to which
 it is granting permission is a hallmark of OAuth.

28 ¹⁰ Raible, *supra* n. 8.

1 provides her Twitter username and password only to Twitter. Twitter then sends a “token” to
2 Facebook, essentially confirming to Facebook that the user’s login to Twitter was legitimate.
3 Scopes are one of the “central components” and perhaps even “the first key aspect” of OAuth.

4 65. But as with the old-fashioned way of authorizing a bank account by providing
5 account and routing numbers and waiting for a small deposit, OAuth requires a user to leave the
6 app and be redirected to another site or interface to log in. This supposedly undermines an app’s
7 ability to sign up new users by driving away individuals who decide it is not worth the trouble of
8 dealing with the OAuth process.

9 66. Yodlee’s API purports to solve this problem, but the distinctions between Yodlee’s
10 API and true OAuth underscore the grave risk that Yodlee poses to individuals. *First*, Yodlee does
11 not provide a clear dialogue box outlining the scopes of the permissions that the user is granting
12 to Yodlee or the permissions the user is denying to Yodlee. Indeed, the user has no option to deny
13 Yodlee any permissions at all.

14 67. *Second*, the core principle of OAuth—and what has made it the industry-standard
15 authorization protocol—is that it provides for access to an individual’s data without disclosing the
16 individual’s password to the service requesting authorization. This places the individual in control
17 because she can cut off the service’s access to her data by revoking the service’s OAuth access.
18 Yodlee specifically designed its API to circumvent this protection, deceiving users into providing
19 Defendants with their bank usernames and passwords so that Defendants can use those credentials
20 to collect sensitive financial information on an ongoing basis without giving the individual a way
21 to revoke access to that data. As explained above, Defendants accomplish this by deceiving users
22 into thinking that they are logging into their financial institutions’ app or website, when in fact
23 they are entering their credentials directly into Defendants’ portal.

24 68. Yodlee is capable of integrating OAuth into its API. It has done so in Europe to
25 comply with the European Union’s Second Payment Services Directive. Yet in the United States,
26 Defendants continue to deploy credential-based authentication because, though it falls short of the
27 industry standard, it is a source of immense profit.

28 69. By failing to provide disclosures or obtain users’ consent to collect and sell their

1 sensitive personal data, Defendants violated Plaintiffs' and Class members' privacy rights and
2 state and federal law.

3 **III. YODLEE'S FAILURE TO DISCLOSE VIOLATES SEVERAL PRIVACY LAWS**

4 70. As discussed above, Yodlee's privacy policy only applies to its "direct-to-consumer
5 services and websites." For consumers who access Yodlee's services through one of Yodlee's
6 clients, such as Paypal, Yodlee pushes off the burden of providing adequate disclosures to
7 consumers onto the client. This is an abdication of Defendants' duties under the law.

8 71. In California, several statutes require Defendants to provide clear disclosures to
9 consumers about their conduct, including that they collect and sell consumers' sensitive personal
10 data.

11 72. For example, the California Consumer Privacy Act ("CCPA") protects consumers'
12 personal information from collection and use by businesses without providing proper notice and
13 obtaining consent.

14 73. The CCPA applies to Defendants Envestnet and Yodlee because they individually
15 earn more than \$25 million in annual gross revenue. Additionally, the CCPA applies to Defendants
16 because they buy, sell, receive, or share, for commercial purposes, the personal information of
17 more than 50,000 consumers, households, or devices.

18 74. The CCPA requires a business that collects consumers' personal information, such
19 as Defendants' business, to disclose either "at or before the point of collection . . . the categories
20 of personal information to be collected and the purposes for which the categories of personal
21 information shall be used." Cal. Civ. Code § 1798.100(b).

22 75. Furthermore, "[a] business shall not collect additional categories of personal
23 information or use personal information collected for additional purposes without providing the
24 consumer with notice consistent with this section." *Id.*

25 76. Other state statutes that govern Defendants' disclosures include California's
26 Financial Information Privacy Act ("CalFIPA"), Cal. Fin. Code § 4053(d)(1), and the California
27 Online Privacy Protection Act ("CalOPPA"), Cal. Bus. & Prof. Code § 22575. CalFIPA requires
28 that the language in privacy policies be "designed to call attention to the nature and significance

of the information” therein, use “short explanatory sentences,” and “avoid[] explanations that are imprecise or readily subject to different interpretations.” Cal. Fin. Code § 4053(d)(1). The text must be no smaller than 10-point type and “use[] boldface or italics for key words.” *Id.* In passing CalFIPA, the California legislature explicitly provided that its intent was “to afford persons greater privacy protections than those provided in . . . the federal Gramm-Leach-Bliley Act, and that this division be interpreted to be consistent with that purpose.” Cal. Fin. Code § 4051. *See infra.*

77. CalOPPA requires that an operator of any online service, as defined therein, “conspicuously post” its privacy policy. Cal. Bus. & Prof. Code § 22575. Under the statute, to “conspicuously post” a privacy policy via a text hyperlink, the hyperlink must include the word “privacy,” be “written in capital letters equal to or greater in size than the surrounding text,” or be “written in larger type than the surrounding text, or in contrasting type, font, or color to the surrounding text of the same size, or set off from the surrounding text of the same size by symbols or other marks that call attention to the language.” Cal. Bus. Prof. Code § 22577(b).

78. The Graham Leach Bliley Act (the “GLBA”) and the regulations promulgated thereunder impose strict requirements on financial institutions regarding their treatment of consumers’ private financial data and the disclosure of their policies regarding the same. Defendants are financial institutions subject to those regulations, which include the Privacy of Consumer Financial Information regulations (the “Privacy Rule”), 16 C.F.R. Part 313, re-codified at 12 C.F.R. Part 1016 (“Reg. P”), and issued pursuant to the GLBA, 15 U.S.C. §§ 6801-6803, and the GLBA’s “Safeguards Rule” (16 C.F.R. Part 314).

79. This regulatory scheme has clear requirements for applicable privacy policies. Under those rules, a financial institution “must provide a clear and conspicuous notice that accurately reflects [its] privacy policies and practices.” 16 C.F.R. § 313.4. Privacy notices must be provided “so that each consumer can reasonably be expected to receive actual notice.” 16 C.F.R. § 313.9; 12 C.F.R. § 1016.9. “Clear and conspicuous means that a notice is reasonably understandable and designed to call attention to the nature and significance of the information in the notice.” 16 C.F.R. § 313.3(b)(1); 12 C.F.R. § 1016.3(b)(1). Ways a company can call attention to its privacy policy include “[using] a plain-language heading” (16 C.F.R. § 313.3(b)(2)(ii)(A);

1 “[using] a typeface and type size that are easy to read” (16 C.F.R. § 313.3(b)(2)(ii)(B)); (c) “[using]
 2 boldface or italics for key words” (16 C.F.R. § 313.3(b)(2)(ii)(D)); or (d) “[using] distinctive type
 3 size, style, and graphic devices, such as shading or sidebars,” when combining its notice with other
 4 information (16 C.F.R. § 313.3(b)(2)(ii)(E)). A company must ensure that “other elements on the
 5 web site (such as text, graphics, hyperlinks, or sound) do not distract attention from the notice.”
 6 16 CFR §313(b)(2)(iii). The notice should appear in a place that users “frequently access.” 16 CFR
 7 §313.3(b)(2)(iii)(A), (B). Privacy notices must “accurately reflect[]” the financial institution’s
 8 privacy policies and practices. 16 C.F.R. §§ 313.4 and 313.5; 12 C.F.R. §§ 1016.4 and 1016.5. The
 9 notices must include the categories of nonpublic personal information the financial institution
 10 collects and discloses, the categories of third parties to whom the financial institution discloses the
 11 information, and the financial institution’s security and confidentiality policies. 16 C.F.R. § 313.6;
 12 12 C.F.R. § 1016.6.

13 80. Both GLBA and CalFIPA require that privacy policies provide consumers with an
 14 opportunity to opt out of the sharing of their personal data. 16 C.F.R. § 313.10; Cal. Fin. Code.
 15 §4053(d)(2).

16 81. Defendants violated these statutory and regulatory requirements because they do
 17 not disclose through the Yodlee privacy policy that they collect consumers’ personal information,
 18 let alone the categories of personal information they collect, nor the purposes for which this
 19 information is collected.

20 82. Yodlee’s privacy policy is not “clear and conspicuous.” Indeed, Yodlee has
 21 designed its privacy policy to be wholly inapplicable to consumers like Plaintiffs and Class
 22 members, who access Yodlee’s services through a third party.

23 83. Nor does Yodlee make these necessary disclosures at the “point of collection.” For
 24 example, as discussed above, when consumers connect their bank account to PayPal through
 25 Yodlee, nowhere is it disclosed that Yodlee collects and sells consumers’ sensitive personal data.
 26 All that is disclosed is that “[PayPal] use[s] Yodlee to confirm your bank details and to check your
 27 balance and transaction as needed, which can help your PayPal payments go through.” This is
 28 materially false and misleading in that it does not disclose: (1) that Yodlee collects and sells users’

1 sensitive personal data; (2) the categories of data that Yodlee collects and sells; or (3) the true
 2 purpose for Yodlee's conduct, i.e., to earn monetary compensation by selling Plaintiffs' and Class
 3 members' data to other entities. (Other apps that incorporate the Yodlee API, such as Personal
 4 Capital, do not disclose their use of Yodlee whatsoever.)

5 84. Further, Yodlee's privacy policy provides an insufficient opportunity to opt out,
 6 including because it fails to use the heading "Restrict Information Sharing With Other Companies
 7 We Do Business With To Provide Financial Products And Services." Cal. Fin. Code § 4053
 8 (d)(1)(A).

9 85. In addition to being financial institutions themselves, governed by the GLBA and
 10 CalFIPA, Defendants also received data from other financial institutions. As such, they violated
 11 the following CalFIPA provision as well:

12 **An entity that receives nonpublic personal information**
 13 **pursuant to any exception set forth in Section 4056 shall not use**
 14 **or disclose the information except in the ordinary course of**
 15 **business** to carry out the activity covered by the exception under
 16 which the information was received.

17 Cal. Fin. Code § 4053.5 (emphasis added).

18 86. One of the exceptions noted in Section 4056 allows sharing of nonpublic personal
 19 information "with the consent or at the direction of the consumer." Cal. Fin. Code. § 4056.
 20 Plaintiffs and Class members did not consent to or direct the release of their sensitive nonpublic
 21 personal information for the reasons described herein. But even if they did, Section 4053.5 still
 22 provides that an entity like Yodlee can *only* use such information to carry out the activity *for which*
 23 *the user provided consent*. Defendants' use of the data for any reason other than connecting users'
 24 bank accounts violates this statutory protection.

25 **IV. GOVERNMENT AND INDUSTRY LEADERS AGREE THAT DEFENDANTS'** 26 **CONDUCT IS WRONG, RISKY, DANGEROUS AND BAD FOR CONSUMERS**

27 87. Government and industry leaders agree that Defendants' conduct runs afoul of basic
 28 standards of decency and proper treatment of consumer data.

88. The Consumer Financial Protection Bureau's 2017 Consumer Protection Principles
 for data aggregators like Yodlee provide that such services should not "require consumers to share

1 their account credentials with third parties”—i.e., anyone other than the user or the bank.¹¹ Of
2 course, Defendants do exactly that.

3 89. Likewise, the Consumer Protection Principles provide that the data practices of a
4 company like Yodlee must be “fully and effectively disclosed to the consumer, understood by the
5 consumer, not overly broad, and consistent with the consumer’s reasonable expectations in light
6 of the product(s) or service(s) selected by the consumer.” Defendants’ disclosures were not full
7 and effective, as described above. Defendants’ data practices were likely to and did deceive
8 Plaintiffs and Class members, are overly broad, and are not consistent with consumers’ reasonable
9 expectations, because they are out of proportion to what is necessary to link financial accounts to
10 FinTech apps.

11 90. The Consumer Protection Principles also provide that data access terms must
12 address “access frequency, data scope, and retention period.” Nowhere do Defendants disclose
13 how they access consumers’ data, how much data they gather and how long they keep it—perhaps
14 because consumers would be outraged to hear the answers.

15 91. The Consumer Protection Principles also provide that consumers must be informed
16 of any third parties that access or use their information, including the “identity and security of each
17 such party, the data they access, their use of such data, and the frequency at which they access the
18 data.” Defendants do not disclose this information.

19 92. Major financial institutions and their trade associations have also voiced concerns.
20 In April 2016, J.P. Morgan CEO Jamie Dimon said the bank is “extremely concerned” about
21 “outside parties,” including “aggregators” (like Yodlee), for three reasons: first, “[f]ar more
22 information is taken than the third party needs in order to do its job”; second, “[m]any third parties
23 sell or trade information in a way [users] may not understand, and the third parties, quite often, are
24 doing it for their own economic benefit – not for the customer’s benefit”; and third, “[o]ften this
25 is being done on a daily basis for years after the customer signed up for the services, which they

26 ¹¹ *Consumer Protection Principles: Consumer-Authorized Financial Data Sharing and*
27 *Aggregation*, Consumer Financial Protection Bureau (Oct. 18, 2017),
28 [https://files.consumerfinance.gov/f/documents/cfpb_consumer-protection-principles_data-](https://files.consumerfinance.gov/f/documents/cfpb_consumer-protection-principles_data-aggregation.pdf)
[aggregation.pdf](https://files.consumerfinance.gov/f/documents/cfpb_consumer-protection-principles_data-aggregation.pdf).

1 may no longer be using.”¹² Dimon recommended that users not share their login credentials with
 2 third parties like Yodlee, in part to avoid loss of important indemnification rights: “When [users]
 3 give out their bank passcode, they may not realize that if a rogue employee at an aggregator uses
 4 this passcode to steal money from the customer’s account, the customer, not the bank, is
 5 responsible for any loss. . . . This lack of clarity and transparency isn’t fair or right.” J.P. Morgan
 6 hit the nail on the head in identifying the egregious invasions of privacy that are not simply
 7 incidental to Defendants’ business but lie at the heart of it.

8 93. In 2017, the American Bankers Association (“ABA”) wrote to the CFPB to express
 9 similar concerns.¹³ The ABA stated that “few consumers appreciate the risks presented when they
 10 provide access to financial account data to non-bank fintech companies,” including the risk of
 11 removing such data from the secure bank environment; that “consumers are not given adequate
 12 information or control over what information is being taken, how long it is accessible, and how it
 13 will be used in the future”; that aggregators like Yodlee make “little effort to inform consumers
 14 about the information being taken, how it is being used or shared, how often it is being accessed,
 15 and how long the aggregator will continue to access it”; and that “[c]onsumers assume that data
 16 aggregators take only the data needed to provide the service requested,” but in reality, “too often
 17 it is not the case.”

18 **INJURY AND DAMAGES TO THE CLASS**

19 94. Plaintiffs and Class members have suffered actual harm, injury, damage and loss as
 20 a result of Defendants’ illegal conduct, including but not limited to economic damages and harm
 21 to their dignitary rights. Had Plaintiffs and Class members known the true nature, significance and
 22 extent of Defendants’ data practices, they would not have used Yodlee.

25 ¹² See Jamie Dimon, Chairman and CEO of JPMorgan Chase & Co., Letter to Shareholders,
 (Apr. 6, 2016), <https://www.jpmorganchase.com/corporate/annual-report/2015/>.

26 ¹³ Rob Morgan, Vice President, Emerging Technologies of American Bankers Association,
 Letter Response to Request for Information Regarding Consumer Access to Financial Records
 27 Docket No.: CFPB-2016-0048 (Feb. 21, 2017), [https://www.aba.com/-
 28 /media/documents/comment-letter/aba-comment-cfpb-data-
 aggregators.pdf?rev=a5603ffb382c49059ebab1dfda631abf](https://www.aba.com/-/media/documents/comment-letter/aba-comment-cfpb-data-aggregators.pdf?rev=a5603ffb382c49059ebab1dfda631abf).

I. PLAINTIFFS AND CLASS MEMBERS HAVE SUFFERED ECONOMIC DAMAGES

95. Defendants' illegal conduct caused Plaintiffs and Class members to suffer economic damages and loss, including but not limited to: (a) the loss of valuable indemnification rights; (b) the loss of other rights and protections to which they were entitled as long as their sensitive personal data remained in a secure banking environment; (c) the loss of control over valuable property; and (d) the heightened risk of identity theft and fraud.

96. Defendants caused all of these damages when, without actual or constructive notice to Plaintiffs and Class members and without their knowledge or consent, Defendants (1) removed their sensitive personal data from the secure banking environment and (2) sold it to third parties, without exercising any oversight or control over what those entities did with the data.

97. Under federal regulations, a consumer is not liable for unauthorized electronic fund transfers from her financial accounts, subject to certain limits and conditions. *See, e.g.*, 12 C.F.R. § 1005.2(m). But Defendants' conduct eliminates consumers' rights to indemnification under these regulations. If Defendants induced Plaintiffs and Class members to provide their bank credentials to Defendants, and a malicious user subsequently uses those credentials to access and improperly transfer funds from Plaintiffs and Class members' accounts, banks consider that transfer to have been authorized because of the initial provision of the credentials to Defendants. As noted above, J.P. Morgan has expressed concern that consumers do not generally understand that they will be responsible for any such loss. For instance, a theft of \$10,000 from a consumer's account would ordinarily leave a consumer liable for only \$50; but if Defendants' conduct in any way contributes to that unlawful access, the consumer may now be liable for the full \$10,000, a loss in value of \$9,950. By removing Plaintiffs' and Class members' data from the secure bank environment and storing it in their own computer systems, networks or servers, Defendants have destroyed the rights and protections to which Plaintiffs and Class members are otherwise entitled. That amounts to an economic loss to Plaintiffs and Class members.

II. PLAINTIFFS HAVE LOST CONTROL OVER VALUABLE PROPERTY

98. The data that Defendants collect, retain and sell has enormous value both to Defendants and to the Plaintiffs and Class members from whom Defendants illicitly obtain it. First,

1 the data at issue is valuable to Defendants. In 2015, Envestnet announced an acquisition of Yodlee
 2 for \$590 million, based in no small part on the universe of consumer data that Yodlee had
 3 accumulated. Defendants package and sell the data it collects to third party customers, thus
 4 demonstrating that there is an active market for Plaintiffs' and Class members' data. The sheer
 5 size of this mountain of data, as well as Defendants' ability to continue accessing Plaintiffs' and
 6 Class members' transaction histories on an ongoing basis, creates a competitive advantage that
 7 Defendants may exercise over their competitors. All of these facts indicate that the data Defendants
 8 gather is valuable. Once Defendants acquire the data, however, Plaintiffs and Class members have
 9 no control over what Defendants do with it, including how they package it and to whom they sell
 10 it. Further, even Defendants exercise no oversight or control over this data after they sell it. Thus,
 11 Plaintiffs and Class members suffered economic loss from the loss of control over their valuable
 12 property.

13 **A. INCREASED RISK OF IDENTITY THEFT AND FRAUD**

14 99. Defendants' conduct not only destroyed Plaintiffs' and Class members' rights to
 15 indemnification in the event their accounts are compromised but has also increased the risk of just
 16 such an incident occurring. As the ABA has recognized, the "sheer volume and value of the
 17 aggregated data" warehoused at entities like Defendants makes them "a priority target for criminals,
 18 including identity thieves." Databases like Defendants' create a one-stop shop for such malicious
 19 actors to gain access to all of a consumer's accounts, creating a "rich reward for a single hack."
 20 Defendants' consolidation of risk to consumers at a single point of entry creates tangible, economic
 21 injury to Plaintiffs and Class members, who must spend time and money closely monitoring their
 22 credit reports and other financial records for any evidence that their accounts have been
 23 compromised. Defendants' conduct has permanently impaired the integrity of Plaintiffs' and Class
 24 members' bank accounts and the banking information and data therein. Plaintiffs and Class
 25 members face an expanded and imminent risk of economic harm from unauthorized transfers,
 26 identity theft, and fraud.

B. PLAINTIFFS AND CLASS MEMBERS HAVE A REASONABLE EXPECTATION OF PRIVACY

100. Plaintiffs’ and Class members’ expectation of privacy in their highly sensitive personal data, which Defendants collected, sold, or otherwise misused, is enshrined in California’s Constitution. Article I, section 1 of the California Constitution provides: “All people are by nature free and independent and have inalienable rights. Among these are enjoying and defending life and liberty, acquiring, possessing, and protecting property, and pursuing and obtaining safety, happiness, *and privacy*.” Art. I., Sec. 1, Cal. Const. (emphasis added).

101. The phrase “*and privacy*” was added in 1972 after a proposed legislative constitutional amendment designated as Proposition 11. Significantly, the argument in favor of Proposition 11 reveals that the legislative intent was to curb businesses’ control over the unauthorized collection and use of consumers’ personal information, stating in relevant part:

The right of privacy is the right to be left alone. It is a fundamental and compelling interest. It protects **our homes**, our families, our thoughts, our emotions, our expressions, our personalities, our freedom of communion, and our freedom to associate with the people we choose. **It prevents government and business interests from collecting and stockpiling unnecessary information about us and from misusing information gathered for one purpose in order to serve other purposes or to embarrass us.**

Fundamental to our privacy is the ability to control circulation of personal information. This is essential to social relationships and personal freedom. The proliferation of government and business records over which we have no control limits our ability to control our personal lives. Often we do not know that these records even exist and we are certainly unable to determine who has access to them.¹⁴

102. Consistent with the language of Proposition 11, numerous studies examining the collection of consumers’ personal data confirm that the surreptitious taking of personal, confidential, and private information from millions of individuals, as Yodlee has done here, violates expectations of privacy that have been established as general social norms.

¹⁴ Ballot Pamp., Proposed Amends. to Cal. Const. with arguments to voters, Gen. Elec. (Nov. 7, 1972) at 27 (emphasis added).

103. Privacy polls and studies uniformly show that the overwhelming majority of Americans consider one of the most important privacy rights to be the need for an individual's affirmative consent before a company collects and shares its users' personal data.

104. For example, a recent study by *Consumer Reports* shows that 92% of Americans believe that internet companies and websites should be required to obtain consent before selling or sharing their data, and the same percentage believe internet companies and websites should be required to provide consumers with a complete list of the data that has been collected about them. Moreover, according to a study by *Pew Research*, a majority of Americans, approximately 79%, are concerned about how data is collected about them by companies.

105. Defendants failed to disclose that they collected, sold, and otherwise misused consumers' sensitive personal data, and failed to obtain consent to do so. This constitutes a violation of Plaintiffs' and Class members' privacy interests, including those enshrined in the California Constitution.

III. YODLEE DOES NOT HAVE ADEQUATE SAFEGUARDS TO PROTECT CONSUMERS' DATA

106. Yodlee claims that "[p]rotecting the personal information of those who use our services is [their] top priority" and that it employs "leading industry standards of de-identification processing," and "technical, administrative, and contractual measures to protect consumers' identities, such as prohibiting analytics and insights users from attempting to re-identify any consumers from the data."¹⁵ These statements are false.

107. According to leaked documents obtained by *Vice News*, Yodlee's data anonymization process involves "removing names, email addresses, and other personally identifiable information (PII) from the transaction data."¹⁶ This includes "masking patterns of numbers such as account numbers, phone numbers, and SSNs and replacing them with 'XXX'

¹⁵ See VICE, *supra* n. 4.

¹⁶ *Id.*

symbols” and “mask[ing] the financial institution’s name in the transaction description.”¹⁷

108. However, Yodlee’s customers (and potential identify thieves) still receive a wealth of information that can be used to re-identify an individual. For example, even Yodlee’s “masked” information still provides a unique identifier for who made the purchase, the amount of the transaction, date of sale, the city, state and zip code of the business where the purchase was made, and other metadata, including primary and secondary merchant fields, that can be combined to identify the specific individual involved in each transaction.

109. Moreover, because Yodlee keeps a unique identifier for each individual consumer in its data set, and these identifiers are preserved across all transactions, marketers (and cybercriminals) can de-anonymize the data by linking multiple transactions by the same user and combining that information with other publicly available data.

110. As Yves-Alexandre de Montjoye, an associate professor at Imperial College London explained, this data is mere “pseudonymized” than anonymized, meaning that while “it doesn’t contain information that’d directly identify a person such as names or email addresses . . . someone with access to the dataset and some information about you . . . might be able to identify you.”

111. Vivek Singh, an associate professor at Rutgers University, raised the same concern, because the data “does not remove spatio-temporal traces of people that can be used to connect back the data to them.” Spatio-temporal traces are metadata associated with the transaction, including the data, merchant, and physical location.

112. Singh and de Montjoye authored a 2015 study published in *Science* in which they successfully identified individuals using a dataset of similar “de-identified” data using three months of transactions covering 1.1 million people.¹⁸ Singh explained with just “three to four” transactions, an attacker “can unmask the person with a very high probability.” The study

¹⁷ *Id.*

¹⁸ Y. de Montjoye, V. Singh et al., *Unique in the Shopping Mall: On the Reidentifiability of Credit Card Metadata*, 357 *SCIENCE* 6221, 536-539 (Jan. 30, 2015), https://science.sciencemag.org/content/347/6221/536?mod=article_inline.

1 concluded that it was possible to determine the identity of an individual from so-called
2 “anonymized” credit card data 90% of the time through simple extrapolation.¹⁹

3 113. Significantly, last year, scientists from the Imperial College London and Université
4 Catholique de Louvain reported that they have developed a model that can re-identify 99.98% of
5 Americans from datasets using as few as fifteen demographic attributes. Notably, these researchers
6 have made their software code available for anyone on the internet.

7 114. Consumers whose information is collected and sold by Yodlee are especially
8 vulnerable because a user’s credit and debit card transactions can reveal a wealth of other personal
9 and demographic information, such as health, sexuality, religion, and political views that can be
10 used to re-identify individuals like Plaintiffs and Class members.

11 115. These studies confirm that Yodlee’s purported “deanonymization” provides little
12 to no protection for Plaintiffs and Class members, given the immense amount of data that Yodlee
13 has been able to collect through its network of over 17,000 connections to financial institutions,
14 billers, reward networks, and other endpoints. As Yodlee’s former chief product officer Peter
15 Hazlehurst explained, Yodlee’s datasets are incredible in size and “can tell you down to the day
16 how much the water bill was across 25,000 citizens of San Francisco or the daily spending at
17 McDonald’s throughout the country.”²⁰

18 116. Furthermore, despite Yodlee’s claim that it employs “technical, administrative, and
19 contractual measures to protect consumers’ identities, such as prohibiting analytics and insights
20 users from attempting to re-identify any consumers from the data,”²¹ Yodlee does not have
21 reasonable safeguards in place to protect consumers’ sensitive personal data.

22 117. Yodlee admitted in a 2015 filing with the SEC that it “does not audit its customers
23 to ensure that they have acted, and continue to act, consistently with such assurances.”²² After
24

25 ¹⁹ *Id.*

26 ²⁰ Hope, *supra* n.1.

27 ²¹ See Vice, *supra* n. 4.

28 ²² *Proxy Statement/Prospectus*, YODLEE, (Oct. 14, 2015),
<https://www.sec.gov/Archives/edgar/data/1337619/000104746915007906/a2226277z424b3.htm>

1 selling consumer data, Yodlee takes no steps to ensure this information remains private, that its
 2 clients are not attempting to re-identify consumers, or use that data for malicious purposes.

3 118. Nor could it. Yodlee's choice not to employ technical safeguards to protect
 4 consumers' sensitive personal data and instead to sell that data to its clients in large text files
 5 removes Yodlee's ability to exert any control over the information once it has been sold.

6 **IV. CONGRESS HAS REQUESTED AN FTC INVESTIGATION INTO ENVESTNET** 7 **& YODLEE PRACTICES**

8 119. Earlier this year, three members of Congress wrote a letter urging the Federal Trade
 9 Commission ("FTC") to investigate Defendants for selling Americans' highly sensitive data
 10 without their knowledge or consent.²³

11 120. In the letter, Senator Ron Wyden, Senator Sherrod Brown, and Representative
 12 Anna Eshoo wrote that "Envestnet [] sells access to consumer data . . . The consumer data that
 13 Envestnet collects and sells is highly sensitive. Consumers' credit and debit card transactions can
 14 reveal information about their health, sexuality, religion, political views, and many other personal
 15 details . . . And the more often that consumers' personal information is bought and sold, the greater
 16 the risk that it could be the subject of a data breach."

17 121. The three members of Capitol Hill were deeply worried that "Envestnet and the
 18 companies to which it had sold data [did not] have the required technical controls in place to protect
 19 Americans' sensitive financial data from re-identification, unauthorized disclosure to hackers or
 20 foreign spies, or other abusive data practices."²⁴

21 122. The letter further warned that:

22 Envestnet does not inform consumers that it is collecting and selling
 23 their personal financial data . . . Instead, Envestnet only asks its
 24 partners, such as banks, to disclose this information to consumers in
 25 their terms and conditions or privacy policy. That is not sufficient
 26 protection for users. Envestnet does not appear to take any steps to
 ensure that its partners actually provide consumers with such notice.
 And even if they did, Envestnet should not put the burden on

27 ²³ See Wyden, *supra* n. 2.

28 ²⁴ *Id.*

consumers to locate a notice buried in small print in a bank's or apps' [sic] terms and conditions . . . in order [to] protect their privacy.

The authors argued that FTC policy prohibits "hid[ing] important facts about how consumer data is collected or shared in the small print of a privacy policy" and FTC has stated that, "companies have an obligation to disclose 'facts [that] would be material to consumers in deciding to install the software.'"

123. According to Envestnet's most recent Form 10-K, in February 2020, the FTC issued a civil investigative demand to Envestnet for various documents related to this matter. Envestnet itself recognizes the risk that as a result of the FTC's investigation, proceedings may be initiated and they may be found to have violated applicable laws, which could have a material adverse effect on their operations and financial condition.

TOLLING, CONCEALMENT AND ESTOPPEL

124. The statutes of limitation applicable to Plaintiffs' claims are tolled as a result of Defendants' knowing and active concealment of their conduct alleged herein. Among other things, Defendants design their software to deceive users into thinking that they are interacting directly with their banks when providing log in credentials to facilitate a connection between their bank accounts and a third-party service. Defendants also fail to disclose to each individual user—either through their own privacy policy, website, or other document—that they store the bank log in information provided in such log in transactions and use those credentials to collect financial data from the individual's bank accounts on an ongoing basis, even though the individual never consented to such data collection. Nor do Defendants inform each individual user that this data collection will continue even if the individual revokes the permissions granted to the third-party service it sought to connect to her bank account. By these actions, Defendants intentionally concealed the nature and extent of their data collection operation to maximize profits resulting from the sale of Plaintiffs' and Class members' highly sensitive financial information. To the extent the Defendants' customers or others made statements regarding Defendants' service or its privacy policies, Defendants either approved those inadequate statements or failed to timely correct them in service of their ongoing scheme to conceal the true nature of their conduct.

125. Plaintiffs and Class members could not, with due diligence, have discovered the

1 full scope of Defendants' conduct, due to Defendants' deliberate efforts to conceal it. All
 2 applicable statutes of limitation also have been tolled by operation of the discovery rule. Under the
 3 circumstances, Defendants were under a duty to disclose the nature and significance of their data
 4 and privacy policies and practices but did not do so. Defendants therefore are estopped from
 5 relying on any statute of limitations.

6 126. Further, this Complaint alleges a continuing course of unlawful conduct by which
 7 Defendants have inflicted continuing and accumulating harm within the applicable statutes of
 8 limitations.

9 127. Each time Defendants engaged in an unlawful act complained of here, Defendants
 10 undertook an overt act that has inflicted harm on Plaintiffs and other members of the Classes.

11 128. For these reasons, the statutes of limitations have been tolled with respect to the
 12 claims of Plaintiffs and members of the Classes asserted in this Complaint.

13 129. Defendants' fraudulent concealment and omissions are common to Plaintiffs and
 14 all Class members.

15 **CLASS ACTION ALLEGATIONS**

16 130. Plaintiffs bring this action pursuant to Federal Rule of Civil Procedure 23
 17 individually and on behalf of the following Classes:

18 **Nationwide Class:** All natural persons in the United States whose
 19 accounts at a financial institution were accessed by Yodlee using
 20 login credentials obtained through Yodlee's software incorporated
 21 in a mobile or web-based fintech app that enables payments
 (including ACH payments) or other money transfers from 2014
 through the present.

22 **California Class:** All natural persons in California whose accounts
 23 at a financial institution were accessed by Yodlee using login
 24 credentials obtained through Yodlee's software incorporated in a
 mobile or web-based fintech app that enables payments (including
 ACH payments) or other money transfers from 2014 through the
 present.

25 131. Excluded from each of the Classes are: (1) any Judge or Magistrate presiding over
 26 this action and any members of their families; (2) Defendants, Defendants' subsidiaries, parents,
 27 successors, predecessors, and any entity in which a Defendant or its parent has a controlling
 28 interest and their current or former employees, officers, and directors; and (3) Plaintiffs' counsel

1 and Defendants' counsel.

2 132. **Numerosity:** The exact number of members of the Classes is unknown and
3 unavailable to Plaintiffs at this time, but individual joinder in this case is impracticable. The
4 Classes likely consist of millions of individuals, and the members can be identified through
5 Defendants' records.

6 133. **Predominant Common Questions:** The Classes' claims present common
7 questions of law and fact, and those questions predominate over any questions that may affect
8 individual Class members. Common questions for the Classes include, but are not limited to, the
9 following:

- 10 a. Whether Defendants violated Plaintiffs' and Class members' privacy rights;
- 11 b. Whether Defendants' acts and practices complained of herein amount to egregious
12 breaches of social norms;
- 13 c. Whether Defendants' conduct was negligent;
- 14 d. Whether Defendants' conduct was unlawful;
- 15 e. Whether Defendants' conduct was unfair;
- 16 f. Whether Defendants' conduct was fraudulent;
- 17 g. Whether Plaintiffs and the Class members are entitled to equitable relief, including
18 but not limited to, injunctive relief, restitution, and disgorgement;
- 19 h. Whether Plaintiffs and the Class members are entitled to actual, statutory, punitive
20 or other forms of damages, and other monetary relief; and
- 21 i. Whether Plaintiffs and the Class members are entitled to actual, statutory, punitive
22 or other forms of damages, and other monetary relief.

23 134. **Typicality:** Plaintiffs' claims are typical of the claims of the other members of the
24 Classes. The claims of Plaintiffs and the members of the Classes arise from the same conduct by
25 Defendants and are based on the same legal theories.

26 135. **Adequate Representation:** Plaintiffs have and will continue to fairly and
27 adequately represent and protect the interests of the Classes. Plaintiffs have retained counsel
28 competent and experienced in complex litigation and class actions, including litigations to remedy

1 privacy violations. Plaintiffs have no interest that is antagonistic to those of the Classes, and
2 Defendants have no defenses unique to any Plaintiff. Plaintiffs and their counsel are committed to
3 vigorously prosecuting this action on behalf of the members of the Classes, and they have the
4 resources to do so. Neither Plaintiffs nor their counsel have any interest adverse to those of the
5 other members of the Classes.

6 136. **Substantial Benefits:** This class action is appropriate for certification because class
7 proceedings are superior to other available methods for the fair and efficient adjudication of this
8 controversy and joinder of all members of the Classes is impracticable. This proposed class action
9 presents fewer management difficulties than individual litigation, and provides the benefits of
10 single adjudication, economies of scale, and comprehensive supervision by a single court. Class
11 treatment will create economies of time, effort, and expense and promote uniform decision-making.

12 137. Plaintiffs reserve the right to revise the foregoing class allegations and definitions
13 based on facts learned and legal developments following additional investigation, discovery, or
14 otherwise.

15 **CALIFORNIA LAW APPLIES TO THE NATIONWIDE CLASS**

16 138. California's substantive laws apply to every member of the Nationwide Class,
17 regardless of where in the United States the Class member resides. The State of California has
18 sufficient contacts to Defendants' relevant conduct for California law to be uniformly applied to
19 the claims of the Nationwide Class.

20 139. Further, California's substantive laws may be constitutionally applied to the claims
21 of Plaintiffs and the Nationwide Class under the Due Process Clause, 14th Amend. § 1, and the
22 Full Faith and Credit Clause, Art. IV § 1 of the U.S. Constitution. California has significant
23 contacts, or significant aggregation of contacts, to the claims asserted by Plaintiffs and all Class
24 members, thereby creating state interests that ensure that the choice of California state law is not
25 arbitrary or unfair.

26 140. Yodlee's headquarters and principal place of business is located in California.
27 Defendants also own property and conduct substantial business in California, and therefore
28 California has an interest in regulating Defendants' conduct under its laws. Defendants' conduct

1 originated in, and emanated from, California and impacted a significant percentage of California
 2 residents, rendering the application of California law to the claims here constitutionally
 3 permissible.

4 141. The application of California laws to the Nationwide Class is also appropriate under
 5 California's choice of law rules because California has significant contacts to the claims of
 6 Plaintiffs and the proposed Nationwide Class, and California has a greater interest in applying its
 7 laws here than any other interested state.

8 **CLAIMS FOR RELIEF**

9 **FIRST CLAIM FOR RELIEF**

10 **Common Law Invasion of Privacy – Intrusion Upon Seclusion** 11 **(On Behalf of Plaintiffs and the Classes)**

12 142. Plaintiffs re-allege and incorporate the preceding allegations of this Complaint with
 13 the same force and effect as if fully restated herein.

14 143. Defendants intruded upon Plaintiffs and Class members' seclusion by (1) collecting,
 15 retaining and selling their sensitive personal data in which they had a reasonable expectation of
 16 privacy; and (2) in a manner that was highly offensive to Plaintiffs and Class members, would be
 17 highly offensive to a reasonable person, and was an egregious violation of social norms.

18 144. Defendants' conduct violated Plaintiffs' and Class members' interests by collecting,
 19 selling, and otherwise misusing their sensitive personal data, including information concerning
 20 private financial transactions (i.e., their informational privacy rights), as well as their interests in
 21 making intimate personal decisions or conducting personal activities without observation,
 22 intrusion, or interference (i.e., their autonomy privacy rights). Defendants' conduct is especially
 23 egregious as they fail to have any adequate security measures in place to control what their clients
 24 do with Plaintiffs' and Class members' information once it is sold, such as re-identifying Plaintiffs
 25 and Class members or using it for nefarious purposes.

26 145. The surreptitious taking and disclosure of personal, confidential, and private
 27 information from millions of individuals was highly offensive because it violated expectations of
 28 privacy that have been established by general social norms.

1 146. Polls and studies consistently show that the overwhelming majority of Americans
2 believe one of the most important privacy rights is the need for an individual's affirmative consent
3 before personal data is shared. For example, one study by *Pew Research* found that 93% of
4 Americans believe it is important to be in control of who can get information about them.

5 147. Defendants' conduct would be highly offensive to a reasonable person in that it
6 violated federal and state laws designed to protect individual privacy, in addition to social norms.

7 148. Defendants intentionally engaged in the misconduct alleged herein for their own
8 financial benefit unrelated to any service they provide. Specifically, Defendants collected and sold
9 Plaintiffs' and Class members' lucrative (and private) sensitive information for their own financial
10 benefit.

11 149. As a result of Defendants' actions, Plaintiffs and Class members have suffered harm
12 and injury, including but not limited to an invasion of their privacy rights.

13 150. Plaintiffs and Class members have been damaged as a direct and proximate result
14 of Defendants' invasion of their privacy and are entitled to just compensation.

15 151. Plaintiffs and Class members are entitled to appropriate relief, including
16 compensatory damages for the harm to their privacy and dignitary interests, loss of valuable rights
17 and protections, heightened risk of future invasions of privacy, and mental and emotional distress.

18 152. Plaintiffs and Class members are entitled to an order requiring Defendants to
19 disgorge profits or other benefits that Defendants acquired as a result of its invasions of privacy.

20 153. Plaintiffs and Class members are entitled to punitive damages resulting from the
21 malicious, willful and intentional nature of Defendants' actions, directed at injuring Plaintiffs and
22 Class members in conscious disregard of their rights. Such damages are needed to deter Defendants
23 from engaging in such conduct in the future.

24 154. Plaintiffs also seek such other relief as the Court may deem just and proper.
25
26
27
28

SECOND CLAIM FOR RELIEF

**Stored Communications Act (“SCA”)
18 U.S.C. § 2701
(On Behalf of Plaintiffs and the Classes)**

155. Plaintiffs re-allege and incorporate the preceding allegations of this Complaint with the same force and effect as if fully restated herein.

156. The SCA provides that a person “providing an electronic communication service to the public shall not knowingly divulge to any person or entity the contents of a communication while in electronic storage by that service[.]” 18 U.S.C. § 2702(a)(1).

157. “Electronic communication” is broadly defined as “any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce[.]” 18 U.S.C. § 2510(12).

158. “Electronic storage” is defined as “any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof; and any storage of such communication by an electronic communication service for purposes of backup protection of such communication[.]” 18 U.S.C. § 2510(17)(A)-(B).

159. “Electronic communication service” is defined as “any service which provides to users thereof the ability to send or receive wire or electronic communications[.]” 18 U.S.C. § 2510(15).

160. “Person” is defined as “any employee, or agent of the United States or any State or political subdivision thereof, and any individual, partnership, association, joint stock company, trust, or corporation.” 18 U.S.C. § 2510(6).

161. Yodlee and Envestnet, as corporations, are persons as defined under 18 U.S.C. § 2510(6).

162. Defendants provide a service that allows Plaintiffs and Class members the ability to send and receive electronic communications from their financial institutions and third-party applications, such as PayPal. Defendants provide this service “to the public” because Defendants’ FinTech and personal financial management technology is incorporated in hundreds of

1 applications used by millions of individuals, including Plaintiffs and Class members.

2 163. Plaintiffs and Class members reasonably expected that Defendants' service did not
3 include accessing, collecting, selling, and otherwise disclosing their "electronic communications,"
4 i.e., their data (as broadly defined), based, in part, on Defendants' failure to provide *any* disclosures
5 or obtain consent for permission to do so.

6 164. Defendants store Plaintiffs' and Class members' electronic communications and
7 intentionally divulged them by selling this information to third parties for monetary compensation,
8 in reckless disregard for Plaintiffs' and Class members' privacy rights for Defendants' own
9 financial benefit.

10 165. Defendants' actions were at all relevant times intentional, willful, and knowing, as
11 evidenced by Defendants accepting monetary compensation in exchange for Plaintiffs' and Class
12 members' electronic communications.

13 166. As a result of Defendants' violations of the SCA, Plaintiffs and Class members
14 have suffered harm and injury, including but not limited to the invasion of their privacy rights.

15 167. Pursuant to 18 U.S.C. § 2707, Plaintiffs and Class members are entitled to: (1)
16 appropriate equitable or declaratory relief; (2) damages, in an amount to be determined at trial,
17 assessed as the sum of the actual damages suffered by Plaintiffs and the Class and any profits made
18 by Defendants as a result of the violation, but in no case less than the minimum statutory damages
19 of \$1,000 per person; and (3) reasonable attorneys' fees and other litigation costs reasonably
20 incurred.

21 **THIRD CLAIM FOR RELIEF**

22 **Unjust Enrichment** 23 **(On Behalf of Plaintiffs and the Classes)**

24 168. Plaintiffs re-allege and incorporate the preceding allegations of this Complaint with
25 the same force and effect as if fully restated herein.

26 169. Defendants received benefits from Plaintiffs and Class members and unjustly
27 retained those benefits at their expense.

28 170. In particular, Defendants received benefits from Plaintiffs and Class members in

1 the form of the sensitive personal data that Defendants collected from Plaintiffs and Class members,
 2 without authorization and proper compensation. Defendants have collected, sold, and otherwise
 3 misused this information, for their own gain, providing Defendants with economic, intangible, and
 4 other benefits, including substantial monetary compensation from the entities who purchased
 5 Plaintiffs' and Class members' sensitive personal data.

6 171. Defendants unjustly retained those benefits at the expense of Plaintiffs and Class
 7 members because Defendants' conduct damaged Plaintiffs and Class members, all without
 8 providing any commensurate compensation to Plaintiffs and Class members.

9 172. The benefits that Defendants derived from Plaintiffs and Class members rightly
 10 belong to Plaintiffs and Class members. It would be inequitable under unjust enrichment principles
 11 in California and every other state for Defendants to be permitted to retain any of the profit or
 12 other benefits it derived from the unfair and unconscionable methods, acts, and trade practices
 13 alleged in this Complaint.

14 173. Defendants should be compelled to disgorge in a common fund for the benefit of
 15 Plaintiffs and Class members all unlawful or inequitable proceeds it received, and such other relief
 16 as the Court may deem just and proper.

17 **FOURTH CLAIM FOR RELIEF**

18 **Violation of Cal. Civ. Code § 1709** 19 **(On Behalf of Plaintiffs and the Classes)**

20 174. Plaintiffs re-allege and incorporate the preceding allegations of this Complaint with
 21 the same force and effect as if fully restated herein.

22 175. California Civil Code § 1709 provides that "[o]ne who willfully deceives another
 23 with intent to induce him to alter his position to his injury or risk, is liable for any damage which
 24 he thereby suffers." A defendant violates §1709 if (i) it had a duty to disclose a material fact to the
 25 plaintiff; (ii) it intentionally concealed that fact with intent to defraud; (iii) plaintiff was unaware
 26 of that fact (and would have acted differently if he were aware), and (iv) plaintiff sustained some
 27 damage as a result.

28 176. California Civil Code § 1710 defines "deceit" as "1. [t]he suggestion, as a fact, of

1 that which is not true, by one who does not believe it to be true; 2. [t]he assertion, as a fact, of that
2 which is not true, by one who has no reasonable ground for believing it to be true; 3. [t]he
3 suppression of a fact, by one who is bound to disclose it, or who gives information of other facts
4 which are likely to mislead for want of communication of that fact; or, 4. [a] promise, made without
5 any intention of performing it.”

6 177. Defendants engaged in various acts of deceit. Defendants either suggested that
7 certain facts are true which they knew were not true or which they had no reasonable grounds to
8 believe were true. For example, when Plaintiffs and Class members link their bank accounts to
9 Paypal through Yodlee, the only disclosure provided is that Yodlee is used “to confirm your bank
10 details and to check your balance and transaction *as needed*, which can help your PayPal payments
11 go through.” This statement is objectively false. Yodlee accesses users’ bank accounts beyond the
12 purposes that it claims. Yodlee actually accesses users’ bank accounts to collect their sensitive
13 personal data and sell it to their customers, well beyond what is necessary to connect users’ bank
14 accounts to PayPal.

15 178. Furthermore, Yodlee suppresses facts and provides other facts that are likely to
16 mislead. For example, Yodlee does not inform consumers that it collects and sells their sensitive
17 personal data. Yodlee improperly relies on its clients to provide necessary disclosures of Yodlee’s
18 own practices and takes no steps to ensure that its clients do so. By failing to disclose these material
19 facts, Plaintiffs and Class members were deceived.

20 179. Defendants willfully engaged in these acts of deceit with intent to induce Plaintiffs
21 and Class members to alter their position to their injury or risk, namely by turning over their
22 sensitive personal data to Defendants under false pretenses.

23 180. Defendants had a duty to disclose these facts to Plaintiffs and Class members; they
24 intentionally concealed those facts with intent to defraud; Plaintiffs and Class members were
25 unaware of these facts, and would have acted differently if they were aware; and Plaintiffs and
26 Class members sustained damage as a result.

27 181. Defendants willfully also engaged in these acts of deceit so that they could access,
28 collect, and sell Plaintiffs’ and Class members’ sensitive personal data for their own personal

benefit, including monetary compensation.

182. Plaintiffs and Class members seek recovery of their resulting damages, including economic damages, restitution, and disgorgement, as well as punitive damages and such other relief as the Court may deem just and proper.

FIFTH CLAIM FOR RELIEF

Violation of California Unfair Competition Law (“UCL”) Cal. Bus. & Prof. Code § 17200 (On Behalf of Plaintiffs and the Classes)

183. Plaintiffs re-allege and incorporate the preceding allegations of this Complaint with the same force and effect as if fully restated herein.

184. Defendants’ conduct as alleged herein constitutes unlawful, unfair, and/or fraudulent business acts or practices as prohibited by the UCL.

185. Defendants’ business acts and practices are “unlawful” under the UCL, because, as alleged above, Defendant violated the California common law, California Constitution, California Civil Code § 1709, the California Consumer Privacy Act, and the Stored Communications Act.

186. Defendants’ business acts and practices are “unfair” under the UCL. California has a strong public policy of protecting consumers’ privacy interests, including protecting consumers’ banking data. Defendants violated this public policy by, among other things, surreptitiously collecting, selling, and otherwise misusing Plaintiffs’ and Class members’ sensitive personal data without Plaintiffs’ and Class members’ consent. Defendants’ conduct violates the policies of the statutes referenced above.

187. Defendants’ business acts and practices are also “unfair” in that they are immoral, unethical, oppressive, unscrupulous and/or substantially injurious to consumers. The gravity of the harm of Defendants’ secretly collecting, selling, and otherwise misusing Plaintiffs’ and Class members’ sensitive personal data is significant, and there is no corresponding benefit resulting from such conduct. Finally, because Plaintiffs and Class Members were completely unaware of Defendants’ conduct, they could not have possibly avoided the harm.

188. Defendants’ business acts and practices are also “fraudulent” within the meaning of the UCL. Defendants have amassed a large collection of sensitive personal data without

complete disclosure and therefore without consumers' knowledge or consent. Defendants' business acts and practices were likely to, and did, deceive members of the public including Plaintiffs and Class members into believing this data was private and only used as necessary, such as to connect users' bank accounts to third party applications. In fact, such information was not private, as Defendants secretly collected, sold, and otherwise misused it for their own purposes.

189. Had Plaintiffs and Class members known that their information would be collected, sold, and otherwise misused for Defendants' benefit, they would not have used Defendants' services.

190. Plaintiffs and Class members have a property interest in their sensitive personal data. By surreptitiously collecting, selling, and otherwise misusing Plaintiffs' and Class members' information, Defendants have taken property from Plaintiffs and Class members without providing just or any compensation.

191. Plaintiffs and Class members have lost money and property as a result of Defendants' conduct in violation of the UCL and seek restitution on behalf of themselves and Class members. Additionally, Plaintiffs and Class members are entitled to an order enjoining Defendants from engaging in the unlawful conduct alleged in this claim and requiring Defendants to delete Plaintiffs' and Class members sensitive personal data, to cease further collection of Plaintiffs' and Class members sensitive personal data, and other appropriate equitable relief, including but not limited to improving its privacy disclosures and obtaining adequately informed consent.

SIXTH CLAIM FOR RELIEF

Request for Relief Under the Declaratory Judgment Act 28 U.S.C. § 2201, *et seq.* (On Behalf of Plaintiffs and the Classes)

192. Plaintiffs re-allege and incorporate the preceding allegations of this Complaint with the same force and effect as if fully restated herein.

193. Under the Declaratory Judgment Act, 28 U.S.C. §§ 2201, *et seq.*, this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and grant further necessary relief. Furthermore, the Court has broad authority to restrain acts, such as here,

1 that are tortious and that violate the terms of the federal and state statutes described in this
2 complaint.

3 194. An actual controversy has arisen in the wake of Defendants' collection, offer for
4 sale, and other misuse of Plaintiffs' and Class members' sensitive personal data without their
5 consent as alleged herein in violation of Defendants' common law and statutory duties.

6 195. Plaintiffs and Class members continue to suffer injury and damages as described
7 herein as Defendants continue to collect, sell, and misuse Plaintiffs' and Class members' sensitive
8 personal data.

9 196. Pursuant to its authority under the Declaratory Judgment Act, this Court should
10 enter a judgment declaring, among other things, the following:

- 11 a. Defendants continue to owe a legal duty to not collect, sell, and misuse
12 Plaintiffs' and Class members' sensitive personal information under, *inter*
13 *alia*, the common law, California Constitution, California Civil Code
14 § 1709, and the California Consumer Privacy Act.
- 15 b. Defendants continue to breach their legal duties by continuing to monitor,
16 collect, and misuse Plaintiffs' and Class members' sensitive personal data;
17 and
- 18 c. Defendants' ongoing breaches of their legal duty continue to cause
19 Plaintiffs and Class members harm.

20 197. The Court should also issue corresponding injunctive relief, including but not
21 limited to enjoining Defendants from engaging in the unlawful conduct alleged in this complaint
22 and requiring Defendants to delete Plaintiffs' and Class members' sensitive personal data, cease
23 further collection of Plaintiffs' and Class members sensitive data, stop selling Plaintiffs' and Class
24 members' sensitive data, and other appropriate equitable relief, including but not limited to
25 providing privacy disclosures and obtaining adequately informed consent.

26 198. If an injunction is not issued, Plaintiffs and Class members will suffer irreparable
27 injury and lack an adequate legal remedy in the event of Defendants' ongoing conduct.

28 199. Federal and state laws prohibit, among other things, the unlawful collection,

1 offering for sale, and other misuse of sensitive personal data without consent. California
 2 specifically recognizes privacy as a fundamental right. The risk of continued violations of federal
 3 and California law is real, immediate, and substantial. Plaintiffs and Class members do not have
 4 an adequate remedy at law because many of the resulting injuries are reoccurring, and Plaintiffs
 5 and Class members will be forced to bring multiple lawsuits to rectify the same conduct.

6 200. The hardships to Plaintiffs and Class members if an injunction is not issued exceed
 7 the hardships to Defendants if an injunction is issued. On the other hand, the cost to Defendants of
 8 complying with an injunction by complying with federal and California law and by ceasing to
 9 engage in the misconduct alleged herein is relatively minimal, and Defendants have a pre-existing
 10 legal obligation to avoid invading the privacy rights of consumers.

11 201. Issuance of the requested injunction will serve the public interest by preventing
 12 ongoing monitoring, collection, and misuse of sensitive personal data without consent, thus
 13 eliminating the injuries that would result to Plaintiffs and the Class.

14 **SEVENTH CAUSE OF ACTION**

15 **Violation of California's Comprehensive Data Access and Fraud Act ("CDAFA"),** 16 **Cal. Pen. Code § 502** **(On Behalf of Plaintiffs and the Classes)**

17 202. Plaintiffs re-allege and incorporate the preceding allegations of this Complaint with
 18 the same force and effect as if fully restated herein.

19 203. Plaintiffs bring this claim on behalf of themselves and the Nationwide Class or, in
 20 the alternative, the California Class, under California law.

21 204. A person violates the CDAFA if it commits one of 14 acts.

22 205. A person violates Cal. Penal Code § 502(c)(1) if it "[k]nowingly accesses and
 23 without permission alters, damages, destroys, or otherwise uses . . . any data, computer, computer
 24 system, or computer network in order to either (A) devise or execute any scheme or artifice to
 25 defraud, deceive or extort, or (B) wrongfully control or obtain money, property or data." (Emphasis
 26 added.) Defendants violated § 502(c)(1) when it accessed Plaintiffs' and Class members' sensitive
 27 personal information and damaged and used Plaintiffs' and Class members' sensitive personal
 28 information. Defendants acted without permission for the reasons described herein. Plaintiffs and

1 Class members had no notice, whether actual or constructive, that Defendants were a separate
 2 entity from the FinTech Apps, and thus no notice that Defendants were operating; had no way to
 3 remove Defendants' software; and do not have an opportunity to consent to Defendants' access to
 4 their sensitive personal data each time that Defendants access it. Defendants accessed and used
 5 this data in order to execute their scheme to defraud and deceive, because Defendants employed
 6 fraud and deceit to induce Plaintiffs and Class members to turn over their financial institution login
 7 credentials to Defendants. Additionally, Defendants accessed and used this data to wrongfully
 8 obtain money, property or data, both because it obtained the data under false pretenses and because
 9 it used the data to develop analytics products that it then sold.

10 206. A person violates Cal. Penal Code § 502(c)(2) if it “[k]nowingly *accesses* and
 11 *without permission* takes, copies, or *makes use of any data* from a computer, computer system, or
 12 computer network.” (Emphasis added.) Defendants violated § 502(c)(2) when they accessed
 13 Plaintiffs’ and Class members’ sensitive personal information without permission as described
 14 herein, and made use of Plaintiffs’ and Class members’ sensitive personal information without
 15 permission as described herein.

16 207. A person violates Cal. Penal Code § 502(c)(3) if it “[k]nowingly *and without*
 17 *permission* *uses or causes to be used computer services*.” (Emphasis added.) Defendants violated
 18 § 502(c)(3) when they knowingly and without permission used or caused to be used the computer
 19 services of Plaintiffs’ and Class members’ financial institutions, as described herein.

20 208. A person violates Cal. Penal Code § 502(c)(4) if it “[k]nowingly *accesses and*
 21 *without permission* adds, alters, *damages*, deletes, or destroys any data, computer software, or
 22 computer programs which reside or exist internal or external to a computer, computer system, or
 23 computer network.” (Emphasis added.) Defendants violated § 502(c)(4) when they knowingly
 24 damaged Plaintiffs’ and Class members’ sensitive personal data, and damaged Plaintiffs’ and Class
 25 members’ financial institutions’ computers, computers systems and computer networks, as
 26 described herein. Defendants acted without permission for the reasons described herein.

27 209. A person violates Cal. Penal Code § 502(c)(6) if it “[k]nowingly *and without*
 28 *permission* *provides or assists in providing a means of accessing* a computer, computer system, or

1 computer network in violation of this section.” (Emphasis added.) Defendants violated § 502(c)(6)
 2 when they knowingly used Plaintiffs’ and Class members’ login credentials, which they obtained
 3 under false pretenses, and provided them to Plaintiffs’ and Class members’ financial institutions,
 4 as described herein. Defendants acted without permission for the reasons described herein.

5 210. A person violates Cal. Penal Code § 502(c)(7) if it “[k]nowingly and without
 6 permission accesses or causes to be accessed any computer, computer system, or computer
 7 network.” (Emphasis added.) Defendants violated § 502(c)(7) when they knowingly used Plaintiffs’
 8 and Class members’ login credentials, which they obtained under false pretenses, to access the
 9 computers, computer systems and computer networks of Plaintiffs and Class members’ financial
 10 institutions, as described herein. Defendants acted without permission for the reasons described
 11 herein.

12 211. Defendants accessed the data, computers, computer systems and computer
 13 networks above in ways that circumvented technical or code-based barriers.

14 212. Plaintiffs and Class members are owners of the sensitive personal data that
 15 Defendants collected, retained and sold, and suffered actual harm, injury, damage and loss as a
 16 result of Defendants’ conduct, as described herein. Thus, Plaintiffs and Class members may bring
 17 a civil action for compensatory damages, including “expenditure[s] reasonably and necessarily
 18 incurred . . . to verify that . . . data was or was not altered, damaged or deleted by access.” Cal.
 19 Pen. Code § 502(e)(1). Further, Defendants shall pay punitive and/or exemplary damages because
 20 their violations were willful. *Id.* § 502(e)(4). Plaintiffs shall be entitled to reasonable attorney’s
 21 fees. *Id.* § 502(e)(2). Plaintiffs also seek such other relief as the Court may deem just and proper.

22 **EIGHTH CAUSE OF ACTION**

23 **Violation of California’s Anti-Phishing Act of 2005** 24 **Cal. Bus. & Prof. Code § 22948.2** **(On Behalf of Plaintiffs and the Classes)**

25 213. Plaintiffs incorporate the substantive allegations contained in all prior and
 26 succeeding paragraphs as if fully set forth herein.

27 214. Plaintiffs brings this claim on behalf of themselves and the Nationwide Class or, in
 28 the alternative, the California Class.

1 215. The California Anti-Phishing Act of 2005 (the “Anti-Phishing Act”) makes it
2 unlawful to use the Internet “to solicit, request, or take any action to induce another person to
3 provide identifying information by representing itself to be a business without the authority or
4 approval of the business.” Cal. Bus. & Prof. Code § 22948.2. “Identifying information” includes
5 bank account numbers, account passwords, and “[a]ny other piece of information that can be used
6 to access an individual’s financial accounts.” Cal. Bus. & Prof. Code § 22948.1(b). An individual
7 who is adversely affected by a violation of Section 22948.2 may bring an action. Cal. Bus. & Prof.
8 Code § 22948.3(a)(2).

9 216. As described herein, Defendants violated the Anti-Phishing Act by representing
10 themselves to be Plaintiffs’ and Class members’ financial institutions. Defendants fraudulently
11 and deceitfully impersonated those institutions in order to induce Plaintiffs and Class members to
12 provide their login credentials to Defendants, as described herein. Defendants did so without
13 obtaining the authority or approval of each financial institution.

14 217. Plaintiffs and Class members have been adversely affected by Defendants’
15 violations of the Anti-Phishing Act because Defendants engaged in this deceitful conduct in order
16 to extract from Plaintiffs and Class members their login credentials and all of the transaction
17 history and other data accessible with those credentials, as detailed above. Defendants caused
18 actual injury, harm, damage and loss to Plaintiffs and Class members for the reasons described
19 herein.

20 218. Plaintiffs and Class members are entitled to relief under Cal. Bus. & Prof. Code
21 § 22948.3(a)(2), including \$5,000 per violation, which damages should be trebled because
22 Defendants engaged in a pattern and practice of violating § 22948.2 (indeed, it is the essence of
23 Defendants’ business model); an injunction against further violations; costs of suit and reasonable
24 attorney’s fees; and such other relief as the Court may deem just and proper.

NINTH CAUSE OF ACTION

**Violation of the Computer Fraud and Abuse Act
18 U.S.C. § 1030
(On Behalf of Plaintiffs and the Classes)**

219. Plaintiffs incorporate the substantive allegations contained in all prior and succeeding paragraphs as if fully restated herein.

A. VIOLATIONS OF 18 U.S.C. § 1030(A)(2)

220. A person violates 18 U.S.C. § 1030(a)(2) if it “intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains—(A) information contained in a financial record of a financial institution . . . [or] (C) information from any protected computer.” Protected computers include computers “exclusively for the use of a financial institution . . . or . . . used by . . . a financial institution . . . and the conduct constituting the offense affects that use by or for the financial institution,” 18 U.S.C. § 1030(e)(2)(A), or computers “used in or affecting interstate or foreign commerce,” 18 U.S.C. § 1030(e)(2)(B).

221. The computer systems, data storage facilities, or communications facilities that Plaintiffs and Class members’ financial institutions use to store Plaintiffs and Class members’ data are “protected computers” under the statute because they are exclusively for the use of financial institutions or, in the alternative, were affected by Defendants’ conduct, or were used in or affected interstate commerce. Defendants intentionally accessed these protected computers and thereby obtained information contained in the financial institutions’ financial records. Defendants did so without authorization. To the extent that Defendants received any valid authorization, their conduct exceeded that authorization for the reasons described above. *See* 18 U.S.C. 1030(e)(6) (defining the term “exceeds authorized access” to mean “to access a computer with authorization and to use such access to obtain or alter information in the computer that the accessor is not entitled so to obtain or alter”).

B. VIOLATIONS OF 18 U.S.C. § 1030(a)(4)

222. A person violates 18 U.S.C. § 1030(a)(4) if it “knowingly and with intent to defraud, accesses a protected computer without authorization, or exceeds authorized access, and by means of such conduct furthers the intended fraud and obtains anything of value, unless the object of the

1 fraud and the thing obtained consists only of the use of the computer and the value of such use is
2 not more than \$5,000 in any 1-year period.”

3 223. Defendants knowingly accessed protected computers, and did so without
4 authorization or in excess of authorization, for the reasons described herein.

5 224. Defendants acted with intent to defraud because they devised a scheme to deceive
6 Plaintiffs and Class members into thinking that they were providing their banking credentials
7 directly to their bank, when in fact they were providing those credentials to Defendants. Through
8 that conduct, Defendants furthered their fraud and obtained things of value, namely, Plaintiffs and
9 Class members’ sensitive personal data.

10 **C. VIOLATIONS OF 18 U.S.C. § 1030(a)(5)(A)**

11 225. A person violates 18 U.S.C. § 1030(a)(5)(A) if it “knowingly causes the
12 transmission of a program, information, code, or command, and as a result of such conduct,
13 intentionally causes damage without authorization, to a protected computer.”

14 226. Defendants knowingly caused the transmission of a program, information, code or
15 command every time it sent Plaintiffs’ and Class members’ credentials to their financial
16 institutions. Defendants did so without authorization for the reasons described herein. Defendants
17 caused damage for the reasons described herein.

18 **D. VIOLATIONS OF 18 U.S.C. § 1030(a)(5)(B), (C)**

19 227. A person violates 18 U.S.C. § 1030(a)(5)(B) if it “intentionally accesses a protected
20 computer without authorization, and as a result of such conduct, recklessly causes damage.” A
21 person violates 18 U.S.C. § 1030(a)(5)(C) if it “intentionally accesses a protected computer
22 without authorization, and as a result of such conduct, causes damage and loss.”

23 228. Plaintiffs’ and Class members’ financial institutions’ computer systems, data
24 storage facilities, or communications facilities are protected computers under the statute for the
25 reasons described herein. Defendants acted without authorization for all of the reasons described
26 herein. Defendants acted not only recklessly but intentionally for all of the reasons herein.
27 Defendants caused damage or loss for the reasons described herein.
28

E. VIOLATIONS OF 18 U.S.C. § 1030(a)(6)

229. A person violates 18 U.S.C. § 1030(a)(6) if it “knowingly and with intent to defraud traffics . . . in any password or similar information through which a computer may be accessed without authorization, if—(A) such trafficking affects interstate or foreign commerce.” The term “traffic” means “transfer, or otherwise dispose of, to another, or obtain control of with intent to transfer or dispose of.” 18 U.S.C. § 1029(e)(5).

230. Defendants acted knowingly and with intent to defraud for the reasons described herein. Defendants acted without authorization for the reasons described herein. Defendants trafficked in passwords and similar information when they obtained control of banking credentials from millions of distinct financial accounts with the intent of transferring them to their own massive database of user information, thus allowing Defendants access to Plaintiffs’ and Class members’ financial institutions’ computers. In the alternative, Defendants trafficked in passwords and similar information when, after acquiring Plaintiffs’ and Class members’ login credentials under false pretenses and using them to login to those individuals’ financial institutions, those institutions sent access tokens to Defendants, which access tokens Defendants then transferred to their app clients or partners.

231. On information and belief, because of the locations of Defendants, their servers, and the millions of accounts for which Defendants acquired credentials and data, Defendants’ trafficking activities affected interstate or foreign commerce.

F. DEFENDANTS CAUSED ECONOMIC LOSS IN EXCESS OF \$5,000, AS WELL AS OTHER DAMAGE

232. Plaintiffs may bring a private right of action for economic damages resulting from Defendants’ violation of the CFAA, provided that Defendants caused “loss to 1 or more persons during any 1-year period . . . aggregating at least \$5,000 in value.” 18 U.S.C. 1030 (c)(4)(A)(i)(I). The CFAA defines the term “damage” to include “any impairment to the integrity or availability of data, a program, a system, or information.” 18 U.S.C. § 1030(e)(8). The CFAA defines the term “loss” to include “any reasonable cost to any victim, including the cost of responding to an offense, conducting a damage assessment, and restoring the data, program, system, or information to its

condition prior to the offense, and any revenue lost, cost incurred, or other consequential damages incurred because of interruption of service.” 18 U.S.C. § 1030(e)(11).

233. Each of the violations detailed above caused economic loss to Plaintiffs and Class members that exceeds \$5,000 per year individually or in the aggregate. In particular, Defendants caused losses to Plaintiffs and Class members by imposing unreasonable costs on them, including the cost of conducting damage assessments, restoring the data to its condition prior to the offense, and consequential damages they incurred by, inter alia, spending time conducting research to ensure that their identity had not been compromised and accounts reflect the proper balances.

234. Defendants’ violations damaged Plaintiffs and Class members in other ways as described herein. Plaintiffs seek such other relief as the Court may deem just and proper.

235. Plaintiffs bring this cause of action within two years of the date of the discovery of their damages. Thus, this action is timely under 18 U.S.C. § 1030(g).

TENTH CAUSE OF ACTION

Violation of Article I, Section I of the California Constitution (On Behalf of Plaintiff Szeto and the California Class)

236. Plaintiffs re-allege and incorporate the preceding allegations of this Complaint with the same force and effect as if fully restated herein.

237. The California Constitution expressly provides for and protects the right to privacy of California citizens: “All people are by nature free and independent and have inalienable rights. Among these are enjoying and defending life and liberty, acquiring, possessing, and protecting property, and pursuing and obtaining safety, happiness, and privacy.” Cal. Const., art. I, § 1.

238. Plaintiff Szeto and members of the California Class have a reasonable expectation of privacy in their confidential financial affairs, including without limitation in the personal information and banking data maintained at their financial institutions. Plaintiffs and California Class members reasonably expected that their login credentials, account numbers, balances, transaction history, and other information was private and secure within the institutions at which they maintain accounts. They reasonably expected that their information and data (a) would be protected and secured against access by unauthorized parties; (b) would not be obtained by

1 unauthorized parties; (c) would not be transmitted or stored outside of the secure bank
2 environment; and (d) would not be sold or used without their knowledge or permission.

3 239. Plaintiff Szeto and California Class members have a legally protected privacy
4 interest in preventing the unauthorized access, dissemination, sale, and misuse of their sensitive
5 and confidential banking information and data.

6 240. Defendants intentionally violated Plaintiff Szeto and California Class members'
7 privacy interests. Defendants intruded upon Plaintiff Szeto and California Class members'
8 sensitive and confidential banking information in a manner sufficiently serious in nature, scope,
9 and actual or potential impact to constitute an egregious breach of the social norms underlying the
10 privacy right.

11 241. Defendants intentionally violated Plaintiff Szeto and California Class members'
12 privacy interests by improperly accessing, downloading, transferring, selling, storing and using
13 their private banking information and data.

14 242. Defendants' violations of Plaintiffs' and California Class members' privacy
15 interests would be highly offensive to a reasonable person, especially considering (a) the highly
16 sensitive and personal nature of Plaintiffs' and California Class members' banking information
17 and data; (b) the extensive scope of data obtained by Defendants, including years of historical
18 transactional data; (c) Defendants' intent to profit from Plaintiffs' and California Class members'
19 data by selling it outright and using it to develop further products and services; and (d) the fact that
20 Defendants used subterfuge to intrude into Plaintiffs' and California Class members' banks' secure
21 environment for the purpose of collecting their data. Defendants' intrusions were substantial and
22 constituted an egregious breach of social norms.

23 243. Plaintiff Szeto and California Class members did not consent to Defendants'
24 violations of their privacy interests.

25 244. Plaintiff Szeto and California Class members suffered actual and concrete injury as
26 a result of Defendants' violations of their privacy interests. Plaintiffs and California Class
27 members are entitled to appropriate relief, including damages to compensate them for the harm to
28 their privacy interests, loss of valuable rights and protections, heightened risk of future invasions

1 of privacy, and the mental and emotional distress and harm to human dignity interests caused by
 2 Defendants' invasions, as well as disgorgement of profits made by Defendants as a result of its
 3 violations of their privacy interests.

4 245. Plaintiff Szeto and California Class members also seek punitive damages because
 5 Defendants' actions—which were malicious, oppressive, and willful—were calculated to injure
 6 Plaintiffs and California Class members and made in conscious disregard of Plaintiffs' and
 7 California Class members' rights. Punitive damages are warranted to deter Defendants from
 8 engaging in future misconduct.

9 **PRAYER FOR RELIEF**

10 WHEREFORE, Plaintiffs on behalf of themselves and the proposed Classes respectfully
 11 request that the Court enter an order:

- 12 A. Certifying the Classes and appointing Plaintiffs as Class Representatives;
- 13 B. Finding that Defendants' conduct was unlawful as alleged herein;
- 14 C. Awarding declaratory relief against Defendants;
- 15 D. Awarding such injunctive and other equitable relief as the Court deems just and proper;
- 16 E. Awarding Plaintiffs and the Class members statutory, actual, compensatory, consequential,
 17 punitive, and nominal damages, as well as restitution and/or disgorgement of profits
 18 unlawfully obtained;
- 19 F. Awarding Plaintiffs and the Class members pre-judgment and post-judgment interest;
- 20 G. Awarding Plaintiffs and the Class members reasonable attorneys' fees, costs, and expenses,
 21 including expert costs; and
- 22 H. Granting such other relief as the Court deems just and proper.
- 23
- 24
- 25
- 26
- 27
- 28

DEMAND FOR JURY TRIAL

Plaintiffs demand a trial by jury for all issues so triable.

Dated: October 21, 2020

/s/ Aaron M. Sheanin

Aaron M. Sheanin (SBN 214472)
Christine S. Yun Sauer (SBN 314307)
ROBINS KAPLAN LLP
46 Shattuck Square, Suite 22
Berkeley, CA 94704
Telephone: (650) 784-4040
Facsimile: (650) 784-4041
asheanin@robinskaplan.com
cyunsauer@robinskaplan.com

Kellie Lerner (*pro hac vice* forthcoming)
David Rochelson
ROBINS KAPLAN LLP
399 Park Avenue, Suite 3600
New York, NY 10022
Telephone: (212) 980-7400
Facsimile: (212) 980-7499
klerner@robinskaplan.com
drochelson@robinskaplan.com

Thomas J. Undlin (*pro hac vice* forthcoming)
ROBINS KAPLAN LLP
800 LaSalle Avenue, Suite 2800
Minneapolis, MN 55402
Telephone: (612) 349-8500
Facsimile: (612) 339-4181
tundlin@robinskaplan.com

Christian Levis
Amanda Fiorilla
LOWEY DANNENBERG, P.C.
44 South Broadway, Suite 1100
White Plains, NY 10601
Telephone: (914) 997-0500
Facsimile: (914) 997-0035
clevis@lowey.com
afiorilla@lowey.com

Anthony M. Christina
LOWEY DANNENBERG, P.C.
One Tower Bridge
100 Front Street, Suite 520
West Conshohocken, PA 19428
Telephone: (215) 399-4770
Facsimile: (914) 997-0035
achristina@lowey.com

1 John Emerson (*pro hac vice* forthcoming)
2 **EMERSON FIRM, PLLC**
3 2500 Wilcrest Drive
4 Suite 300
5 Houston, TX 77042
6 Telephone: (800) 551-8649
7 Facsimile: (501) 286-4659
8 jemerson@emersonfirm.com

9 Robert Kitchenoff (*pro hac vice* forthcoming)
10 **WEINSTEIN KITCHENOFF & ASHER LLC**
11 150 Monument Road, Suite 107
12 Bala Cynwyd, PA 19004
13 Telephone: (215) 545-7200
14 kitchenoff@wka-law.com

15 Adam Frankel (*pro hac vice* forthcoming)
16 **GREENWICH LEGAL ASSOCIATES LLC**
17 881 Lake Avenue
18 Greenwich, CT 06831
19 Telephone: (203) 622.6001
20 afrankel@grwlegal.com

21 *Attorneys for Plaintiffs and the Proposed Classes*
22
23
24
25
26
27
28